高等学校理科教材

近世代數

熊全淹 编著



武汉大学出版社

GROUPS
RINGS
FIELDS
MODULES



高等学校理科教材

近世代数

熊全淹　编著

武汉大学出版社
1995

近　世　代　数

熊全淹　编著

*

武汉大学出版社出版
（430072　武昌　珞珈山）
湖北省通山县印刷厂印刷
（437600　湖北省通山县通羊镇南市路165号）
新华书店湖北发行所发行

*

850×1168　1/32　11.875印张　301千字
1963年10月上海科技第1版　1978年8月上海科技第2版
1984年9月本社第1版　　1991年12月本社第2版
1999年8月第2版第8次印刷
印数：18001－21000
ISBN 7-307-00856-4/O·74
定价：10.80元

范德瓦尔登氏名著《近世代数学》1937年再版后，武汉大学故教授萧君绛先生率先译教并自筹资出版。熊全淹教授师承萧先生留校授《代数学》多年，其讲稿屡经推敲、修改、增删逐渐形成本书。在本社新2版中增设模与代数一章并尽可能在适当的地方兼蓄若干近代发展的成果。前四章介绍群、环、体、模的基础理论，后四章再作深入的论述。全书注重阐明思路、详尽推理、深入浅出、顺其自然。在所谓“代数化”的今天，尤利于初学者用。

本书获1988年国家教委高等学校优秀教材二等奖。

责任编辑　夏天安

封面设计　马重慧

内容提要

本书系统地介绍近世代数的基本理论.全书共八章.前四章对群、环、体、模的基础理论作一般的介绍,后四章则作进一步较深入的论述.每节后附有习题,每章后列有参考文献.书末附有习题解答,供读者参考.

本书叙述由浅入深,推理详尽,便于阅读,可作为高等院校数学系大学生和研究生近世代数课的教材或教学参考书,也可供广大教师和数学工作者参考.

第二版前言

这次修改主要是充实模的内容，除在新增加的第 4 章 § 4.1 中系统地介绍外，在其他有关章节也适当补充，目的在介绍模的最基本的概念及性质，供读者阅读其他代数参考书之用. 因为在本书对模的引用不多，所以不作更多的论述. 此外简化了某些定义，改写了某些证明，改正了一些错误，还适当增补了一些内容，各章都有变动，大小不一.

新添了第 4 章，其中第 2 节是从以前的 § 4.4 搬来的，其它章节仍旧没有变动. 这样全书共 8 章，前 4 章是群、环、体、模的基本介绍，后 4 章是它们较深入的论述.

这次改动承副教授谭季伟同志提出了很多宝贵意见，使本书生色不少，附此志谢.

熊全淹

1990 年 12 月，时年八十

于珞珈山武汉大学

第一版前言

本书较系统、全面地介绍近世代数的基本理论. 作为高等院校数学系学生的基础读本，在内容选择上，力求简明扼要，避免涉及一些过于艰深的问题，以求达到加深基础理论的认识. 在次序编排上，大体参照范德瓦尔登著《近世代数学》一书.

本书自成系统，论述由浅入深，推理详尽，读者不必参考其它书籍就可顺利阅读. 每节后附有习题，有些习题提出了一些重要概念和问题，读者宜加注意. 书末附有解答，供读者校核. 每章后列出了适当的参考文献，其中有些表明近代发展情况，也有不少选自Amer. Math. Monthly 杂志上的短文；后者内容大都不太困难，读者如有可能，望选择阅读，以加深基本功的训练，增强解决问题的能力.

本书是根据多年来武汉大学数学系的《近世代数讲义》改编而成. 1963 年第一版和 1978 年第二版都由上海科学技术出版社出版，此次第三版则由武汉大学出版社出版. 他们对本书出版的鼓励和支持，编者表示衷心感谢.

这次改版变动较大，主要是简化了一些定理的证明、添加了一些内容、改正了发现的错误、改写了某些节段，但仍保留了全书的结构. 本书屡经修改，质量虽有所提高，但限于编者水平，缺点和错误仍在所难免，敬请读者惠予指正.

本书初版、二版以来，承蒙广大读者爱护，提出了不少宝贵意见，使得本书在修订改版中得以改进，在此一并谨表谢忱.

熊全淹

1983 年 10 月

于珞珈山武汉大学

目　　录

第1章

基本概念

这章简单地介绍集合、映射、分类等基本概念，并且解释记号 $\in,\subset,\supset,\cap,\cup,\{\cdots\}$ 等的意义，作为以后各章的准备.

§1.1 集　　合

数学中讨论的对象，如代数中的数、矩阵，几何中的点、直线等，我们现在统统叫做**元素**，有时就简单地叫做**元**. 若干个（有穷个或无穷多个）元的集体，叫做**集合**，或简单地叫做**集**.

我们要知道一个集，必定要知道其中所有的元，也就是说，我们对于任意一个元，要能够判别它是否在这个集中. 譬如，所有整数组成一个集，因为我们随便拿一个数来，都可以判别它是否是整数，这个集又叫做**整数集**，我们用 $\mathbf{Z}$ 来表示.

一个集都有自己的特性，譬如，整数集中任意元，都有整数这个特性. 平面上所有点组成的集与平面上所有圆组成的集都各有各的特性. 因此，对于一个集，我们可以用它的特性来判别任意元是否在它里面.

任意一个元 a，如果它有集合 M 的特性，也就是说，它是 M 中元时，我们就用记号

$$a\in M$$

来表示. 如果它没有集合 M 的特性，也就是说，它不是 M 中元时，我们就用

$$a\overline{\in} M$$

来表示. 有时, a 在 M 中我们也说 a 属于 M, 或者说 M 包含 a. 同样, a 不在 M 中我们也说 a 不属于 M, 或者说 M 不包含 a. 一个集所包含的元假如是有穷个, 就叫做**有穷集**, 否则就叫做**无穷集**. 一个集所包含的元的个数, 叫做这集的**元数**或**浓度**. 有穷集的元数当然是正整数.

集合可以用列举其中所有元来表示, 譬如, 整数集 $\mathbf{Z}$ 可以写成 $\mathbf{Z}=\{0,1,-1,2,-2,\cdots\}$, 或

$$\mathbf{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}.$$

一般, 假如 M 含元 $a,b,c,\cdots$, 我们就用记号表为

$$M=\{a,b,c,\cdots\}.$$

通常一个集都含有一个以上的元, 但是当它只含一个元时, 这个集就与它所含的那唯一一个元常常不加区别. 为了叙述方便, 我们便假定不包含任何元的也成为一个集, 叫做**空集**, 它的元数是零. 譬如, 大于 1 而小于 2 的整数集合就是空集.

假如集合 N 中所有元都是集合 M 中元, 也就是说, N 是 M 的一部分, 或者说, 任意一个元, 如果它有 N 的特性, 它一定也有 M 的特性, 那么 N 就叫做 M 的**子集**, M 又叫做 N 的**包含集**. 我们用记号 $N\subseteq M$ 或 $M\supseteq N$ 表示. 子集与包含集的关系可以用图形(图 1.1)来说明.

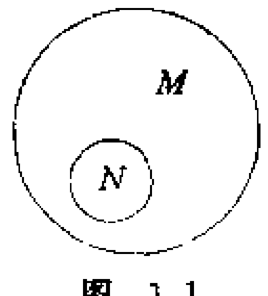


图 1.1

有穷集的子集是有穷集, 无穷集的包含集又是无穷集.

为了方便, 我们假定任意集都包含空集. 再从 $A\subseteq B$ 及 $B\subseteq C$, 我们就得到 $A\subseteq C$.

假如 M 中所有元都属于 N, 同时 N 中所有元又都属于 M, 即

$$M\subseteq N,\quad N\subseteq M,$$

也就是说, M 与 N 的特性完全相同时, 我们就说 M 与 N **相等**, 用记号

$$M=N$$

表示. 假如 $N\subseteq M$，但 M，N 不相等，那么 N 就叫做 M 的**真子集**，M 叫做 N 的**真包含集**，用记号

$$N\subset M \text{ 或 } M\supset N$$

表示，这时 N 中所有元都属于 M，但 M 中至少有一个元不属于 N.

上面，我们介绍了集合的基本概念，现在介绍它的三个结合法.

定义 1 假如 M，N 是两个集，那么属于 M 同时又不属于 N 的所有元形成的集 D，叫做 M 与 N 的**差集**，用记号

$$D=M-N$$

表示.

图 1.2

D 是 M 的子集，我们可以用图形(图 1.2)中 M 中的阴影部分来说明.

显然

$$M-N\neq N-M.$$

定义 2 假如 M，N 是两个集，那么属于 M 同时又属于 N 的所有元形成的集 P，叫做 M 与 N 的**交集**，用记号

$$P=M\cap N$$

表示.

于是 P 是 M，N 的子集，并且任何集只要它同时是 M，N 的子集，它一定是 P 的子集，因此 P 是包含在 M，N 中的**最大集**. 关于交集的概念，我们可以用图形(图 1.3)来说明.

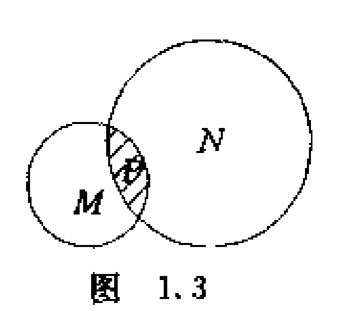


图 1.3

定义 3 假如 M，N 是两个集，那么属于 M 或者属于 N 的所有元形成的集 S，叫做 M 与 N 的**并集**，用记号

$$S=M\cup N$$

表示.

于是 S 是 M,N 的包含集,并且任何集只要它同时是 M,N 的包含集,它一定也是 S 的包含集,因此 S 是包含 M,N 的最小集.关于并集的概念,我们可以用图形(图1.4)来说明.

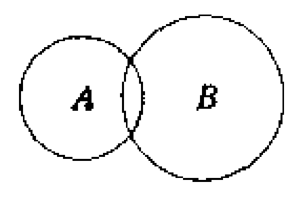


图 1.4

由定义,我们容易得知 $N\cap(M-N)$ 是空集,又

$$M=(M\cap N)\cup(M-N).$$

假如 A,B,C 是三个集,显然

$$(A\cap B)\cap C=A\cap(B\cap C),$$
$$(A\cap B)\cap C=(A\cap C)\cap(B\cap C),$$
$$(A\cup B)\cup C=A\cup(B\cup C),$$
$$(A\cup B)\cup C=(A\cup C)\cup(B\cup C).$$

下面是关于交集与并集的两个分配律.

定理 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C).$

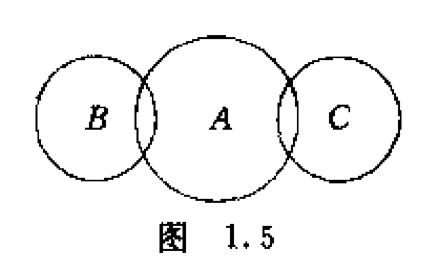


图 1.5

用图形说明如左.

证明 首先因为

$$B\subseteq B\cup C,$$

所以 $A\cap B\subseteq A\cap(B\cup C)$.

同样 $A\cap C\subseteq A\cap(B\cup C)$,因此

$$(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C).$$

再假如 $a\in A\cap(B\cup C)$,那么 $a\in A$,$a\in B\cup C$. 于是 $a\in B$ 或 $a\in C$. 从前者言,$a\in A\cap B$;从后者言,$a\in A\cap C$. 因此 $a\in(A\cap B)\cup(A\cap C)$,这就是说

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C),$$

所以定理成立.

同样我们有

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C).$$

为了区别,由元组成的集,叫做**第一层集**,把第一层集当作元

组成的集,叫做第二层集.第二层集又常叫做系.

若干个集的交集与并集可以按两个集的情形同样定义.假定L是由集A、B,C,…组成的系,我们用

$$A\cap B\cap C\cap\cdots$$

表示L的交集,用

$$A\cup B\cup C\cup\cdots$$

表示L的并集.要注意的是L虽然是第二层集,但它的交集、并集却都是第一层集.

习　题　1.1

1. 任意两个集是否都有交集与并集?

2. 假定$A\subseteq B$,那么$A\cup B=$? $A\cap B=$?

3. 假定A,B,C是三个集,试证:

(i)　$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$;

(ii)　$(A-B)\cup(B-A)=(A\cup B)-(A\cap B)$.

4. 假定A,B,C是三个集,如果它们的乘法规定是

$$AB=(A\cup B)-(A\cap B),$$

试证:$(AB)C=A(BC)$.

5. 假定M是元数为n的有穷集,L是M的所有子集组成的系,试证:L的元数是2^n.

§1.2　映射、分类

我们知道,近世代数中集合的元是抽象的,因此,两个集合如何进行比较是一个重要问题.映射这个概念主要用途之一就是用来解决这个问题,它是近世代数中最基本的工具.

下面是一些最基本概念.

对于集M中每一个元a,如果根据某种规则,我们可以使它与集N中唯一一个元对应,那么这对应叫做M射到N的**映射**,那个与a对应的元,叫做a的**像**,a又叫做它的像的**像源**.这时M中

任意元在 N 中都有像，但 N 中任意元在 M 中不一定都有像源. 如果 N 中元在 M 中不都有像源，那么这映射叫做 M 射到 N **内的映射**. 如果 N 中任意元在 M 中都有像源，那么这映射叫做 M 射到 N **上的映射**. 有时又叫做**满射**.

假如 M 射到 N 的映射用 σ 来表示，那么 a 的像，我们就用 $\sigma(a)$ 来表示，有时这映射又表为 $a\to\sigma(a)$. 映射这个概念与数学分析中函数的概念一致，因此 $\sigma(a)$ 又常叫做 a 的**函数**.

显然，M 射到 N 内的映射就是 M 射到 N 中某个子集上的映射. 譬如在整数集 $\mathbf{Z}$ 中，根据自乘这个规则，把任意整数 a 与它的自乘 a^2 对应，即 $a\to a^2$，那么这对应是 $\mathbf{Z}$ 射到自己内的映射，也是 $\mathbf{Z}$ 射到由所有整数平方组成的子集上的映射.

我们知道，对于映射 σ，像源 a 固然只有唯一的像 $\sigma(a)$，但是像 $\sigma(a)$ 就不一定只有一个像源 a，它可能有一个以上的像源. 任意像只有一个像源的映射，又叫做**一对一的映射**；有时叫做**单射**，不是一对一的映射，又叫做**多对一的映射**. 假如 σ 是 M 射到 N 的映射，B 是 N 的子集，A 是 M 中所有这样元组成的子集，它们的像都在 B 中，那么 A 叫做 B 对于映射 σ 的**完全像源**.

M 射到 N 的映射 σ，当 $a_1\neq a_2$ 时，$\sigma(a_1)\neq\sigma(a_2)$，也就是说，当 $\sigma(a_1)=\sigma(a_2)$ 时，$a_1=a_2$，那么 σ 就是单射. 单射又是满射时，有时叫做**双射**.

集合 M 射到 N 的双射 σ 又叫做**可逆映射**，用记号

$$a\longleftrightarrow\sigma(a)$$

表示. 这时 N 中元 b 的像源用 $\sigma^{-1}(b)$ 来表示. 显然 $b\to\sigma^{-1}(b)$ 是 N 射到 M 上的映射，我们叫它做 σ 的**逆映射**，用记号 σ^{-1} 表示. 因此，任意可逆映射都有唯一一个逆映射，这逆映射也是可逆映射. 假如 σ 是可逆映射，那么它的逆映射 σ^{-1} 的逆映射就是 σ，这就是说

$$(\sigma^{-1})^{-1}=\sigma.$$

譬如，在整数集 $\mathbf{Z}$ 中，我们把偶数与 0 对应，奇数与 1 对应，这样就得到 $\mathbf{Z}$ 射到集合 $\{0,1\}$ 上的映射，这映射是多对一的，0 的完

全像源是所有偶数，1 的完全像源是所有奇数，它们都没有唯一的像源. 假如我们把整数 n 与 $2n$ 对应，即 $n\to 2n$，那就得到 $\mathbf{Z}$ 射到偶数集上的映射，这映射是单射，因此它是可逆映射，它的逆映射就是 $2n\to n$.

假如有一个单射把两个集 M、N 中的一个，譬如说 M，射到另一个 N 上，那么这两个集就叫做**有相等的浓度**，或**元数**. 显然 $\mathbf{Z}$ 与偶数集有相等的浓度，因此一个集的浓度也可以与它的真子集的浓度相等，这是无穷集的一个重要性质. 任意有穷集是没有这个性质的. 与正整数集或它的子集有相等浓度的集，叫做**可数集**. 一个集如果不是可数集，就叫做**不可数集**. 任一可数集中元可以用正整数做标号来排列，于是任意可数集 M 可以写成

$$M=\{a_1,a_2,\cdots,a_n,\cdots\}.$$

有穷集是可数集，正整数集是可数集，整数集 $\mathbf{Z}$ 也是可数集. 再可数个可数集的并集又是可数集，因此有理数集是可数集.

假定 $M=N$，那么 M 射到 N 的映射，就叫做 M **射到自己的映射**，M 射到 N 上(内)的映射，就叫做 M **射到自己上(内)的映射**. M 射到自己的双射即 M 的可逆映射，有时又叫做 M 的**变换**. 对于 M 中任意元使自身与它对应，也就是说，不使 M 中任意元变动，是 M 射到自己的双射，叫做 M 的**恒等映射**，用 I 表示，即 $I(a)=a$. 很多重要的映射都是射到自己上的映射，譬如，平面上的旋转就可以看成为平面上的点集射到自己上的映射. 要注意的是 M 射到自己内的映射有时是单射，而 M 射到自己上的映射却有时不是单射. 譬如，映射 $n\to 2n$ 就是一个 $\mathbf{Z}$ 射到自己内的单射，而映射 $2n\to n$，$2n+1\to 2n+1$ 则是一个 $\mathbf{Z}$ 射到自己上的多对一的映射.

假如 σ_1，σ_2 都是 M 射到 N 的映射，如果对于 M 中任意元 a，有 $\sigma_1(a)=\sigma_2(a)$，我们就说这两个映射**相等**，用记号 $\sigma_1=\sigma_2$ 表示. 假如 σ 是 A 射到 B 的映射，τ 是 B 射到 C 的映射，$\sigma(a)=b$，$\tau(b)=c$，即 $a\to b$，$b\to c$，我们容易证明，对应 $a\to c$ 就是 A 射到 C 的映射，叫做映射 τ，σ 的**积**，用记号 $\tau\sigma$ 表示，即

$$\tau\sigma(a)=\tau(\sigma(a)).$$

这就是说，$\tau\sigma$ 是先施行 σ，后施行 τ 得到的映射.

要注意的是，同一个集的任意两个映射的积是存在的，但一般对于不同集的两个映射不一定有积，假如有积，其积也不只一个. 譬如 σ 是 M 射到 N 的映射，τ 是 N 射到 M 的映射，这时，$\tau\sigma$，$\sigma\tau$ 都有意义，但前者是 M 射到自己的映射，而后者则是 N 射到自己的映射，两者显然不一致. 即令 $M=N$，一般 $\tau\sigma$ 与 $\sigma\tau$ 也不一定相等，即 $\tau\sigma\neq\sigma\tau$，也就是说，映射的乘法不适合交换律. 像这样的例子，我们在几何上是常见的. 再假如 σ 是可逆映射，那么 $\sigma^{-1}\sigma(a)=a$，因此 $\sigma^{-1}\sigma=I$，这就是说，$\sigma^{-1}\sigma$ 是恒等映射. 同样，$\sigma\sigma^{-1}$ 也是恒等映射. 再假如 σ，τ 都是可逆映射，那么 $\tau\sigma$，$\sigma\tau$ 又都是可逆映射. 显然 $\sigma^{-1}\tau^{-1}$，$\tau^{-1}\sigma^{-1}$ 就分别是它们的逆映射.

为了方便，映射等式 $\gamma=\tau\sigma$ 有时用**交换图**(图 1.6)来表示. 同样，交换图(图 1.7)表示 $\tau\sigma=\delta\gamma$. 这里所谓的交换是指在图中从一个始点沿着每一条路线到达一个终点所得到的映射都是相等的.

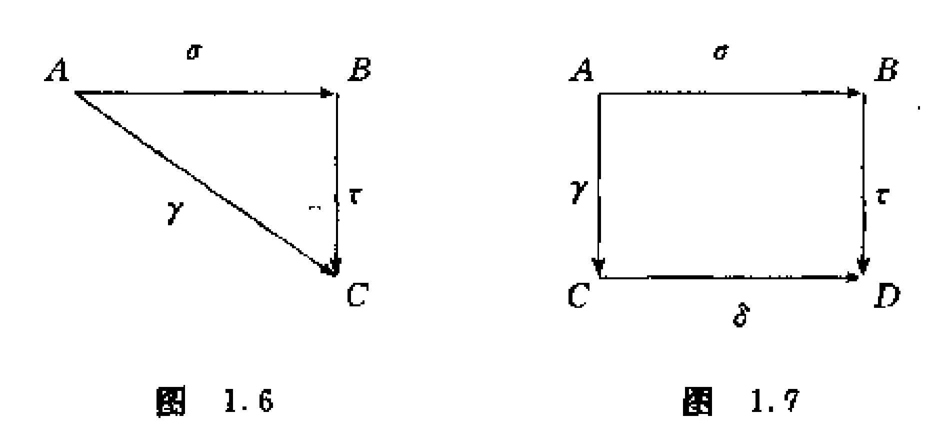


图 1.6　　　　图 1.7

假定对于集 M 中任意两元 a，b，根据某个规则，我们可以把 a，b 与某集中唯一的一个元 c 对应，那么这对应，我们叫做 M 的**结合法**，有时又叫做 M 的**代数运算**. 这时我们又常常说，根据这结合法，可以把 a，b 结合得到元 c，因此我们又说 M 有一个结合法. 譬如，对于整数集 **Z** 中任意两数 a，b，我们命 $a+b$ 与它们对应，那么这对应就是 **Z** 的结合法，它就是普通的加法. 同样，对于 a，b，我们

命 $a \cdot b$ 与它们对应，这对应也是 $\mathbf{Z}$ 的结合法，它就是普通的乘法.

一个集，假如它具有适合某些法则的结合法，或代数运算，就叫做**代数系**. 像上面所示，整数集 $\mathbf{Z}$ 是代数系，因为它的加法、乘法两个结合法适合交换律、结合律、分配律等法则. 近世代数的目的就是讨论某些基本代数系关于结合法的性质，也就是代数性质. 因此可以说，近世代数是研究某些基本代数系的理论学科.

上面我们介绍了映射，现在再来介绍分类这个概念.

我们知道，通常我们把两个元看成为一个元，或者说两个元相等，所用的记号“=”适合下面三个律：

1° 自反律：$a=a$；

2° 对称律：假如 $a=b$，那就 $b=a$；

3° 传递律：假如 $a=b, b=c$，那就 $a=c$.

并且引用等号时也只是引用了这三个律，但是适合这三个律的关系还有很多. 一般来说，我们有：

定义 假如对于一个集中元，规定了一个关系～，并且可以判别其中每对元 a, b 是否有这关系 $a \sim b$，再这关系还适合自反、对称、传递三个律，即

1° $a \sim a$，

2° 假如 $a \sim b$，那就 $b \sim a$，

3° 假如 $a \sim b, b \sim c$，那就 $a \sim c$.

那么这关系，叫做这集的**等价关系**.

譬如，初等几何中的三角形全等、相似都是三角形间的等价关系，但是整数集中不相等，或者大于、小于等关系都不是等价关系. 又如在有穷集 $M=\{1,2,4,6,10\}$ 中，假定两个数的和能够用 4 整除这个关系是～，即当 $4 \mid (a+b)$ 时 $a \sim b$，显然对称律成立. 再我们不难证明传递律也成立，但自反律不成立，因此这关系不是 M 的等价关系[1].

在一个集中，根据某种关系或者用某个观点把某些元看成相

等或同类，把某些元看成不相等或不同类，叫做**分类**. 下面是分类与等价关系之间的一个重要性质.

定理 假如集 M 有一个等价关系，所有与其中一个元等价的元形成的子集，叫做一类，那么 M 就能够分成为若干个这样没有公共元的类而无剩余. 反过来，假如 M 能够分成若干个没有公共元的集而无剩余，这种集我们叫它做类，那么元素在同一类这个关系就是等价关系.

证明 定理的后半段我们容易知其成立，因此，我们只要证明前半段就行了.

假定集 K_a 是 M 中所有与元 a 等价的元形成的类，那么类 K_a 中包含的元是相互等价的，这是因为从 $a\sim b, a\sim c$，根据对称律、传递律就得到 $b\sim c$. 显然 M 中任意元必定属于这样的某一类，因此 M 可以分成这样的类而无剩余.

假如我们能够证明任意这样的两类不是相等就是没有一个公共元，那么 M 中任意一元只能在唯一类，因此定理的前半段就告成立.

假定两类 K_a、K_b 有一个公共元 c，那么 $a\sim c, b\sim c$，因此 $b\sim a$. 如果元 $x\in K_a$，因为 $a\sim x$，所以 $b\sim x$，于是 $x\in K_b$. 因此

$$K_a\subseteq K_b.$$

同样，我们可以证明 $K_b\subseteq K_a$，所以 $K_a=K_b$. 这就是说，任意两类如果不相等，那么它们就没有一个公共元，于是定理的前半段成立，因此定理得证.

于是我们得知一个集，如果有一个等价关系，它就有一种分类. 反过来，如果它有一种分类，它就有一个等价关系.

假如 n 是正整数，在整数集 $\mathbf{Z}$ 中，两数 a,b 的差 $a-b$，如果能够用 n 整除，即 $n\mid(a-b)$ 时，叫做 a 与 b 关于模 n **同余**，用记号

$$a\equiv b \pmod{n} \quad 或 \quad a\equiv b\ (n)$$

表示，有时又简写成 $a\equiv b$. 显然 $a\equiv a$，并且我们容易证明：假如 $a\equiv b$，那么 $b\equiv a$. 再假如 $a\equiv b, b\equiv c$，那么 $a\equiv c$. 所以定是等价关

系.于是对这个关系,整数集 $\mathbf{Z}$ 有一个分类,a 所在的类是所有形如 $a+kn$ (k 是任意整数)的数形成的集,叫做 a 关于 n 的同余类,我们用 $\bar{a}$ 表示,即

$$\bar{a}=\{a+kn \mid k \text{ 是任意整数}\},$$

因此 $\mathbf{Z}$ 可以分成为 n 个类:

$$\bar{0},\ \bar{1},\ \cdots,\ \overline{n-1}.$$

这是因为关于模 n,任意一整数必定与 $0,1,\cdots,n-1$ 中某一数同余,并且 $0,1,\cdots,n-1$ 中任意两数都不同余.当 $n=1$ 时,整个 $\mathbf{Z}$ 成为一类;当 $n=2$ 时,$\mathbf{Z}$ 就分成为两类,一类是所有偶数形成的偶数类,一类是所有奇数形成的奇数类.任意元只与自身同余,并且相异的元都不同余的同余叫做零同余.因此 $\mathbf{Z}$ 自身可以看成是根据零同余的分类,它的每个同余类只有一个元.

上面是为了叙述方便,假定 $n>0$,其实 $n<0$ 时也是同样成立的,这时整数集 $\mathbf{Z}$ 可以分成 $|n|$ 个同余类.

习　题　1.2

1. 假如 $a\equiv b\ (n)$,$c\equiv d\ (n)$,那么

$$a+c\equiv b+d\ (n),\quad a-c\equiv b-d\ (n),$$
$$ma\equiv mb\ (n),\quad ac\equiv bd\ (n).$$

2. 试就 $n=-5$ 时,把整数集 $\mathbf{Z}$ 分类.

3. 假如 σ 是 A 射到 B 上的映射,τ 是 B 射到 A 上的映射,如果 $\sigma\tau=I$,那么 σ 是 τ 的逆映射.

4. 假如 σ 是 M 射到 N 上的映射,A,B 分别是 M,N 的子集,试证:$\sigma(A)$ 的完全像源包含 A,而 B 的完全像源的像就是 B.

5. 有人说从对称律和传递律可以推出自反律,因此自反律可以不要,他的理由是从 $a\sim b$,由对称律得 $b\sim a$,再由传递律便得 $a\sim a$,你的意见如何?

6. 等价三个律可以改成:

(1) $a\sim a$,

(2) 如果 $a\sim b$,$a\sim c$,那么 $b\sim c$.

为什么?

§1.3 自然数、数学归纳法

依照发展的过程来讲，人类首先知道的数是正整数，也就是自然数

$$1,2,3,4,5,\cdots,$$

它们组成的正整数集又叫做**自然数集**. 在这节我们不叙述以它的基本性质为特征的公理[2]，只叙述它的一些基本性质，目的在于介绍数学归纳法的证法和定义，以备以后引用.

一个集，假如有一个叫做某元在某元前的顺序关系，元 a 在元 b 前，我们就说 a 小于 b，或者 b 大于 a，用记号 $a<b$ 或 $b>a$ 来表示，如果这关系又满足下面两个条件：

1° 对于任意两元 a,b，下面的关系必定有一个而且只有一个成立：

$$a=b,\ a<b,\ b<a;$$

2° 对于三元 a,b,c，从 $a<b,b<c$，就有 $a<c$，

那么这集就叫做**有序集**. 空集认为是有序集. 自然数集依数大小的顺序是有序集，这性质有时又叫做**自然数的有序性**.

再自然数集是无穷集，即它的元数不是自然数. 假如其中数依大小的顺序排，那么在任意一数后还有数.

下面是自然数集的另一基本性质，这性质有时又叫做**自然数的最小性**.

定理1 在自然数集的任一非空子集 M 中，必定有一个最小数，也就是说，在集 M 中有不大于其它任意数的数.

证明 因为 M 非空，所以在 M 中可以取一数 n，显然，M 中所有不大于 n 的数组成的非空集 $N\subseteq M$. 如果 N 中有最小数，那么这最小数就是 M 的最小数，但从 1 到 n 只有 n 个自然数，于是 N 中所含的数最多只有 n 个，所以 N 有最小数，因此定理就成立.

根据这性质，我们可以推得下面重要定理，它是数学归纳法原

理的依据.

定理 2　假定 M 是由自然数组成的集，如果它含有 1，并且当它含有数 $n-1$ 时，也含有数 n，那么它含所有的自然数，即 M 是自然数集.

证明　假定 N 是所有不属于 M 的自然数组成的集，如果它是空集，那么定理成立. 假定 N 非空，由上面的定理得知 N 中必定有一个最小数 c，因为 $c\overline{\in} M$，$1\overline{\in} N$，所以 $c\neq 1$，因此 $c-1$ 是自然数. 但 c 是 N 中最小数，所以 $c-1\in M$，于是由假设，$c\in M$. 这与上面的假设矛盾. 因此 N 是空集，也就是说，所有自然数都在 M 中，所以定理得证.

于是我们得知，为了要证明一个命题对于所有自然数都是真实的，我们只要证明两件事，首先证明它对于 1 是真实的，再假定这命题对于自然数 $n-1$ 是真实的时，进而证明它对于自然数 n 也是真实的就行了. 这就是普通所谓的数学归纳法. 此外，数学归纳法还有下面另一形式.

为了要证明一个命题对于所有的自然数都是真实的，我们只要证明它对于 1 是真实的，并且假定它对于所有小于 n 的自然数都是真实的时，再证明它对于自然数 n 也是真实的就行了. 这形式在应用上有时比上面的方便.

譬如，任意一笔大于 7 元的整数付款可以用 3 元及 5 元票面的钞票支付，这一事实可以用数学归纳法验证如下：显然，8 元的付款可以用一张 3 元及一张 5 元的钞票支付，9 元的付款可以用三张 3 元的钞票支付，10 元的付款可以用两张 5 元的钞票支付. 这就是说，当 $n=1,n=2,n=3$，即

$$1+7=8,\quad 2+7=9,\quad 3+7=10$$

时，这事实是真实的；假定小于 n 时这事实是真实的，因为

$$n+7=[(n-3)+7]+3,$$

所以当为 n 时这事实也是真实的，因此对于任意 n 这事实都是真实的，即任意 $n+7$ 元的付款都可以用 3 元及 5 元的钞票支付.

再有许多定义也可以根据归纳法的原理来规定，这就是说，一个定义对于所有的自然数都规定好了，只要根据两件事实，首先我们对于数1规定这定义，其次假定这定义对于自然数 $n-1$（或是小于 n 的所有自然数）已经规定好了，再规定它对于自然数 n 的意义就行了.

譬如，假定一个集有一个乘法的结合法，其中任意 n 个元 a_1，a_2，…，a_n 的乘积

$$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n,$$

我们可以根据归纳法这样来规定它的意义：

$$\prod_{i=1}^{1} a_i = a_1, \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n.$$

习 题 1.3

1. 试用归纳法证明：对于任意自然数 n，

$$4^{n+1} - 3n - 4$$

必定是9的倍数.

2. 试用归纳法原理规定 a^n 的意义，这里 n 是自然数.

参 考 文 献

1 Roseubauw R A. Remark on Equivalence Relation. Amer. Math. Monthly, 1955(62): 650

2 （前苏）勃罗斯库列亚柯夫 N B 著. 数与多项式. 吴品三译. 北京：高等教育出版社. 第三章

第2章

群

这章简单地介绍群的基本概念，主要是说明群、子群、同构、同态、正规子群、商群等的意义，以及它们的基本性质；在第5章中，我们还要进一步讨论它们的一些比较复杂的重要性质.

§2.1 群的概念

在数学各部门以及它的应用中，很多代数系是只有一种结合法的，譬如，后面所述的变换的集合就是这样. 在只有一种结合法的代数系中，最重要的就是群，它的运算法则与数的运算法则类似，并且有非常广泛的应用，是近世代数中最基本的概念.

定义 一个集G，假如它不是空集，并且满足下面4个条件，就叫做群：

1° G有一个闭合的结合法，这就是说，G中任意两元a,b的结合c仍然是G中元. 结合法通常写成乘法，这时c又叫做a,b的积，我们用记号

$$a\cdot b=c \quad 或 \quad ab=c$$

表示. 要注意的是积ab虽然是由a,b唯一决定的，但一般它还与a,b的顺序有关，也就是说，ab不一定等于ba.

2° G的结合法适合结合律，也就是说，对于G中任意三元a,b,c，我们有

$$(ab)c=a(bc).$$

3° G中有一个(左)**单位元**e，对于G中任意元a，有

$$ea=a.$$

4° 对于 G 中任意元 a，在 G 中有一个满足

$$a^{-1}a=e$$

的(左)**逆元** a^{-1}，这里 e 就是上面的(左)单位元.

一个非空集，假如它满足上面的条件 1°，也就是说，它有一个闭合的结合法时，我们就叫它做**乘集**. 假如它满足上面 1°，2°两个条件，我们又叫它做**半群**. 半群也是一个重要概念.

一个群，假如它的结合法还满足交换律：

$$ab=ba,$$

就叫做**交换群**或**阿贝耳**(N. H. Abel，1802—1829)**群**.

群这个概念概括了很多代数系，为了对这概念有较深入的认识，下面给出一些例.

譬如，所有正有理数，结合法是通常的乘法，成一个群，它的单位元是 1. 有理数集 **Q** 对于加法成群，单位元是 0. 但对于乘法只成为半群，而不能成为群，因为零没有逆元. 同样，整数集 **Z** 对加法成群. 又整数 1，－1 或者单独的一个整数 1，对乘法都成群，这些都是交换群. 由 1 个元组成的群，叫做**单位元群**，元数是有穷的群叫做**有穷群**，否则就叫做**无穷群**. 群 G 的元数用 $|G|$ 表示.

又如所有形如 (a,b) 的元的集合 M，其中 a,b 都是实数，并且 $a\neq 0$，如果 $(a,b)(c,d)=(ac,bc+d)$，那么 M 成群，$(1,0)$ 是单位元，(a,b) 的逆元是 $(a^{-1},-ba^{-1})$.

下面，我们再给出两类重要的群，它的元都不是数.

由实数组成的所有 n 阶满秩矩阵对乘法成为群，叫做 K 上的 n 阶线性群，或简称**线性群**，用 $GL(n,K)$ 表示，这里 K 是实数集. 线性群的单位元是对角线上元都是 1 其余都是 0 的单位矩阵，n 维线性空间的所有满秩线性变换对乘法形成的群就是 n 阶线性群.

在空间，绕一个固定点的所有旋转组成一个群，叫做**旋转群**. 这是因为两个旋转 s,t 顺次施行的结果仍然是一个绕那个固定点

的旋转. 假如我们把先施行 t 再施行 s 得到的旋转,叫做 s,t 的积,用 $s\cdot t$ 或 st 表示,那么结合律显然成立. 恒等旋转就是单位元. 一个旋转的逆就是与原旋转相反的旋转. 从几何直观我们很容易得知 st 不一定是 ts,因此旋转群不一定是交换群.

假如空间中所有点的集合用 M 表示,那么绕一个固定点的旋转,显然是 M 射到自己上的可逆映射,也就是 M 的变换. 但变换不一定是旋转,如果把旋转换成更广泛的变换,我们要问,M 的所有变换是否也像上面旋转一样能够形成为群?

因为变换是可逆映射,由 §1.2 我们得知,任意两个变换 s,t 的积 st 仍然是一个变换,它是先施行变换 t,再施行变换 s 得到的变换. 假如 a 是施行的对象,那就有*)

$$st(a)=s(t(a)).$$

要证明结合律 $(rs)t=r(st)$,我们只要把两边的变换同时施行到对象 a 上,这样我们就有

$$(rs)t(a)=(rs)(t(a))=r(s(t(a))),$$
$$r(st)(a)=r(st(a))=r(s(t(a))),$$

因此结合律成立. 恒等变换 I 是把每个施行对象仍然变成自己的映射,即

$$I(a)=a,$$

因此,对于任意变换 s,我们有 $Is=s$,所以恒等变换具有群的单位元的性质. 任意变换 s 都有逆变换 s^{-1},它是把 $s(a)$ 变成为 a 的映射,因此 $s^{-1}s=I$. 从上面看来,集 M 的所有变换满足群的 4 个条件,所以,所有这些变换形成为群,叫做集 M 的**变换群**. 一般它不是交换群. 假如 M 是元数为 n 的有穷集,那么这个变换群也叫做 **n 个文字上的对称群**,或 **n 次对称群**,或者简称为**对称群**,用 S_n 表示. 也就是说,n 个文字上的所有变换组成的群就是对称群 S_n. 我

---

*) 有的书上把 st 看成是先施行 s,再施行 t 得到的变换,这时我们有

$$(a)st=((a)s)t.$$

们容易知道，$|S_n|=n!$．所以 S_n 是有穷群．当 $n>2$ 时，不是交换群．

当 M 是有穷集时，它的变换有时又叫做排列．对于排列，也就是对于对称群的元，下面有一个简明的表示法．

假如 M 是元数为 n 的有穷集，记成 $M=\{1,2,\cdots,n\}$，那么它的排列 s 可以用式子表示如下：

$$s=\begin{pmatrix}1 & 2 & \cdots & n\\ s(1) & s(2) & \cdots & s(n)\end{pmatrix},$$

式中 $s(i)$ 就是它上面 i 的像，譬如，

$$s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$$

是 $\{1,2,3,4\}$ 的一个排列，它把 1 换成 2，2 换成 4，3 不动，4 换成 1．再我们容易知道，

$$s^{-1}=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 3 & 2\end{pmatrix}.$$

又假定 $t=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$，那么

$$st=\begin{pmatrix}2 & 1 & 4 & 3\\ 4 & 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix},$$

同样 $ts=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$.

对称群在代数中是非常重要的．从历史来说，研究群首先是研究对称群，群的抽象化是自弗罗宾纽斯（G. Frobenius，1849—1917）开始的．在第 7 章，我们得知对称群的概念首先是伽罗瓦（E. Galois，1811—1832）[1]建立的，他创造这概念来证明 4 次以上的一般多项式不能够用根号解出．此外，由后面 § 2.4 我们还得知，一个有穷群可以看成是对称群的子群，因此，假如对称群研究清楚了，有穷群也就研究清楚了．

上面给出了群的一些例子，现在我们再从群的定义出发来讨论群的基本性质．

从群定义中条件 2°，我们得知任意三元 a,b,c 的乘积，由它们自身及它们的顺序唯一决定，与结合的先后也就是与所加的“括弧”无关，对于任意 n 个元的乘积也是如此.

定理 1 群 G 中任意 n 个元 $a_1,a_2,\cdots,a_n$ 的乘积由它们自身及它们的顺序唯一决定.

证明 我们用归纳法来证明. 当 $n=3$ 时，就是群定义的条件 2°. 现在假定元数小于 n 时定理成立，来证明元数是 n 时定理也成立.

n 个元依 $a_1,a_2,\cdots,a_n$ 的顺序的乘积不外下列各种形式：

$$(a_1)\cdot(a_2\cdot a_3\cdots a_n),$$
$$(a_1\cdot a_2)\cdot(a_3\cdots a_n),$$
$$\cdots,$$
$$(a_1\cdot a_2\cdots a_{n-1})\cdot(a_n).$$

但其中任意一种

$$\begin{aligned}(a_1\cdot a_2\cdots a_m)(a_{m+1}\cdots a_n)&=(a_1\cdot(a_2\cdots a_m))\cdot(a_{m+1}\cdots a_n)\\&=(a_1)\cdot((a_2\cdots a_m)\cdot(a_{m+1}\cdots a_n))\\&=(a_1)\cdot(a_2\cdots a_n),\end{aligned}$$

这就是说，它们都与第一种一致，所以它们的乘积与所加的括弧无关，因此定理成立.

假如 G 是交换群，那么 $a_1,a_2,\cdots,a_n$ 的乘积由它们自身就唯一决定，与它们的顺序无关.

于是为了方便，n 个元 $a_1,a_2,\cdots,a_n$ 的乘积，我们就用 $a_1a_2\cdots a_n$ 表示，不另加括弧. 此外，与普通代数学中一样，我们又有

$$\underbrace{a\cdots a}_{n\text{个}}=a^n,\ \underbrace{a^{-1}\cdots a^{-1}}_{n\text{个}}=a^{-n},\ a^0=e,\ a^1=a.$$

从群定义中 3°，4°两条件，我们有 $a^{-1}aa^{-1}=ea^{-1}=a^{-1}$；用 a^{-1} 的(左)逆元左乘就得到 $eaa^{-1}=e$，即

$$aa^{-1}=e.$$

也就是说，左逆元同时又是右逆元，因此我们又叫 a^{-1} 做 a 的逆

元. 再因为

$$ae=aa^{-1}a=ea=a,$$

也就是说,左单位元同时又是右单位元,因此我们又叫 e 做单位元.

群的单位元只有唯一的一个,这是因为,假如 e_1,e_2 都是单位元,那就有

$$e_1e_2=e_2=e_1.$$

元 a 的逆元也只有唯一的一个,这是因为,假如 b,c 都是 a 的逆元,那么 $ba=e,ca=e$,因为 $ac=e$,所以

$$b=bac=ec=c.$$

显然,元 a 又是它的逆元 a^{-1} 的逆元,即

$$(a^{-1})^{-1}=a.$$

关于两个元乘积的逆元,我们有下面的计算规则:

$$(ab)^{-1}=b^{-1}a^{-1},$$

这是因为 $(b^{-1}a^{-1})ab=b^{-1}(a^{-1}a)b=b^{-1}b=e$.

假定 a,b 是群 G 的元,那么方程 $ax=b$ 与 $ya=b$ 在 G 中都只有唯一一个解,就是因为

$$a(a^{-1}b)=(aa^{-1})b=eb=b,$$

$$(ba^{-1})a=b(a^{-1}a)=be=b,$$

所以 $x=a^{-1}b,y=ba^{-1}$ 分别是它们的解. 显然,它们的解都是唯一的

我们又常常说 $a^{-1}b$ 是 a 左除 b 的商,ba^{-1} 是 a 右除 b 的商. 因为乘法与因子的顺序有关,所以 a 左除 b 与 a 右除 b,它们的商一般不是相等的. 于是在群中,乘法这种运算是有逆运算的,也就是说,在群中除了乘法运算外,还有它的逆运算除法这种运算,并且对于除法来说,它也与乘法一样是闭合的.

假定 a,b,b' 是群 G 的元,并且 $ab=ab'$ 或 $ba=b'a$,那就有 $b=b'$. 这是因为,用 a^{-1} 左乘 $ab=ab'$ 的两边或用 a^{-1} 右乘 $ba=b'a$ 的两边,就得到 $b=b'$. 因此,群的结合法又是适合消去律的.

下面，我们来讨论群组成的条件.

显然，群定义中 3°，4°两个条件可以引用(右)单位元及(右)逆元而改成为 $ae=a$，$aa^{-1}=e$ 的形式，但是不可改为 $ae=a$，$a^{-1}a=e$.[2]此外，这两个条件还可以用另外的形式来表达.

定理 2 群定义中 3°，4°两个条件，可以用对除法是闭合的，也就是说，对于群中任意元 a,b，方程 $ax=b$，$ya=b$ 在群中有解这条件来代替.

证明 我们只要用群定义中 1°，2°两条件与对除法是闭合的这一条件能够推出群定义中 3°，4°两条件就行了.

假定 c 是群中元，e 是方程 $xc=c$ 的解，即 $ec=c$. 如果 a 是群中任意元，并且 $cy=a$，那么由 $ecy=cy$，即得

$$ea=a.$$

因此，群定义中条件 3°成立. 至于条件 4°，从 $xa=e$ 的可解性就可以推出来，所以定理得证.

由上面的证明，我们得知群中一元如果与群中某元相乘，其积仍然是某元，那么它就是群的单位元. 又，一个集，假如它对于乘法及它的逆运算除法都是闭合的，并且乘法的结合律也成立，那么它就成为群.

定理 3 假如 G 是有穷集，那么它成群所需要的除法是闭合的这条件又可以用消去律来代替.

证明 假定 $G=\{a_1,a_2,\cdots,a_n\}$，a 是 G 中任意元，那么 $\{aa_1,aa_2,\cdots,aa_n\}$ 是 G 的子集，但这 n 个元彼此互异，因为假如 $aa_i=aa_j$，由消去律就得到 $a_i=a_j$，这与假设不合，所以

$$G=\{aa_1,aa_2,\cdots,aa_n\}.$$

因此 G 中任意元 b 可以写成 $b=aa_l$ 的形式，所以 $x=a_l$ 是方程 $ax=b$ 在 G 中的解. 同样，我们可以证明 $b=xa$ 在 G 中也有解，因此定理成立.

于是，我们得知适合消去律的有穷半群是一个群. 但要注意的是有穷是一个重要条件，否则定理不成立，譬如，整数集 **Z** 就是如

此，它对乘法不成群.

群的很多性质可以用来作为它的定义，因此群可以有很多不同的定义，罗伦茨(P. Lorenzen)曾举了40个以上的定义，其中有不用乘法而用除法来定义的，读者如有兴趣，可参考本章末的文献[3].

我们容易知道，一个乘集或一个群，假如其中任意两元的积已经知道，那么这乘集或这群的结合法也就完全知道. 假如乘集 $G=\{a_1,a_2,\cdots,a_n,\cdots\}$，卡莱(A. Cayley，1821—1895)用下面的表来表示 G 中任意两元的结合法，叫做乘法表，当 G 是群时，这表又叫做群表，

	a_1	$\cdots$	a_n	$\cdots$
a_1	a_1a_1	$\cdots$	a_1a_n	$\cdots$
$\vdots$	$\cdots\cdots$			
a_n	a_na_1	$\cdots$	a_na_n	$\cdots$
$\vdots$	$\cdots\cdots$			

譬如，群 $G=\{e,a,b\}$ 中元的结合法为

$$ee=e,\ ea=ae=a,\ eb=be=b,$$
$$aa=b,\ bb=a,\ ab=ba=e.$$

那么它的群表就是

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

从乘法来看元素间的结合法非常明显，因此，我们给出一个群时，常常就给出它的群表. 在群表的每行每列中，群的任意元必定出现一次而且也只能出现一次，这是因为在群中消去法是成立的. 交换群并且只有交换群才有关于主对角线对称的群表.

当群 G 的结合法满足交换律时，也就是说，G 是交换群时，我

们常常把结合法写成加法，积 ab 就写成和 $a+b$，这时 G 又叫做加群，有时也叫做模. 单位元写成 0，叫做零元，元 a 的逆元写成 $-a$，叫做负 a. 即

$$0+a=a,\quad -a+a=0.$$

再

$$\underbrace{a+\cdots+a}_{n个}=na,\ \underbrace{(-a)+\cdots+(-a)}_{n个}=-na.$$

并且我们又常常把 $a+(-b)$ 写成 $a-b$，叫做 a 减 b，因此 $-(a-b)=b-a$. 特别地，当模的元是数时，我们又常常把它叫做数模，因此有理数集 **Q**，整数集 **Z** 都是数模.

习　题　2.1

1. 假如 $\{1,2,3,4\}$ 的乘法表是

	1	2	3	4
1	2	1	4	3
2	4	2	3	1
3	1	3	2	4
4	3	4	1	2

它们是否成为群？假如不成为群，结合律是否成立？有无单位元？

2. 试证下面 4 个矩阵对于乘法成群：

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}-1&0\\0&1\end{pmatrix}.$$

3. 试证下面 6 个分数：

$$r,\ \frac{1}{r},\ 1-r,\ \frac{1}{1-r},\ \frac{r-1}{r},\ \frac{r}{r-1}$$

成群，这时两个分数的结合法是把第 2 个分数代入第 1 个分数中的 r 所得到的结果.

4. 假定 M 是某集合的所有子集的系，如果其中子集 A,B 的结合法 $AB=(A\cup B)-(A\cap B)$，试证：M 成群.

5. 试求 s^2，t^2，st，ts，tst^{-1}，sts^{-1}，假如

$$s=\begin{pmatrix}a&b&c&d&e\\b&e&a&d&c\end{pmatrix},\ t=\begin{pmatrix}a&b&c&d&e\\b&c&a&e&d\end{pmatrix}.$$

6. 试求3个文字上的对称群S_3的群表.

7. 试证:群G为交换群的必要充分条件是对于其中任意两元a,b有

$$(ab)^2=a^2b^2.$$

8. 假如G是群,如果其中任意元的逆元就是它自身,或者说每个元的阶数是2,那么G是交换群.

9. 试证:在任意非交换群中,存在满足$ab=ba$两个异于单位元的元a,b.

10. 假定G是群,a是G中一元,试证:映射$\sigma_a(g)=ag$(或ga),$g\in G$,是G的变换,并且G的所有这样的变换成为一个群.

11. 假定G是非空集合,它有一个叫做除法的闭合的结合法a/b,并且

1° $a/a=b/b=e$, 2° $a/(b/b)=a$, 3° $(a/c)/(b/c)=a/b$.

试证:G对乘法$ab=a/b^{-1}$,$b^{-1}=e/b$成群,其中$a/a=e$是单位元,$e/a=a^{-1}$是a的逆元.

§2.2 子 群

在研究一个群的构造时,也就是说,整个地来看群中元素间的关系时,当然需要考虑它的子群.群的全部内容大都与子群有关,子群是一个重要概念.

定义 一个群G的非空子集H,假如对于G的结合法成为群,就叫做G的**子群**.

譬如,整数集对加法形成的群是有理数集对加法形成的群的子群,但1,-1对乘法形成的群不是有理数集对加法形成的群的子群,因为它们的结合法不一致.

群可以看成自身的子群,异于自身的子群,叫做**真子群**.任一群有只由单位元形成的单位元群做它的子群.一个群的任意多个子群的交集仍然是一个子群,但是任意两个子群的并集一般不成群.

假如H是G的子群,显然H的单位元就是G的单位元,H中元a的逆元也就是a在G中的逆元.

显然,有穷群只能有有穷个子群,它的逆也是成立的,即一个

群如果只有有穷个子群，那么它就是有穷群.

下面，我们首先讨论子集成为子群的条件.

定理 1 群 G 的非空子集 H 成为子群的必要充分条件是:

1° 假如 H 包含元 a,b，那么它也包含它们的积 ab，

2° 假如 H 包含 a，那么它也包含 a 的逆 a^{-1}.

证明 因为必要性是显然的，下面，我们只证明充分性.

上面的条件 1°就是群定义的条件 1°，结合律在 G 中成立，当然在 H 中也同样成立. 再根据上面的条件 2°，我们又得知假如 H 包含 a，它也包含 a^{-1}，因此 H 包含 $a^{-1}a=e$，于是 H 成群，所以定理成立.

上面两个条件，我们把它并合成为一个，就得到

定理 2 群 G 的非空子集 H 成为子群的必要充分条件是：假如 H 包含 a,b，那么 H 也包含 ab^{-1}.

证明 因为如果 H 包含 a，那么它就包含 $aa^{-1}=e$，所以 H 也包含 $ea^{-1}=a^{-1}$. 再如果 H 包含 a,b，它就包含 $a(b^{-1})^{-1}=ab$，因此定理得证.

譬如，线性群 $GL(n,K)$ 中所有行列式为 1 的矩阵形成为子群，叫做**特殊线性群**，用 $SL(n,K)$ 表示，这是因为从 $|A|=1$，$|B|=1$，我们就有 $|A|\cdot|B^{-1}|=1$.

当群是加群时，a 的负元是 $-a$，因此定理 2 中的必要充分条件就是：假如 H 包含 a,b，那么 H 也包含 $a-b$.

特别当 H 是有穷集时，它成为子群的必要充分条件只是定理 1 中的条件 1°. 因为这时，我们可以把消去律来代替群定义中条件 3°，4°，但是消去律在 G 中是成立的，因此在 H 中也同样成立.

我们再来介绍对称群的重要子群——交代群.

我们首先来简化上节中排列的表示. 我们用(1234)表示这样的排列，它是把 1 换成 2，2 换成 3，3 换成 4，最后的 4 换成最前面的 1，其余的文字都不变动，这种排列又常叫做**循环排列**. 由两个文字组成的循环排列，叫做**对换**. 譬如(12)就是把 1 换成 2，2 换成

1，其余的文字都不变动的排列. 为了方便，我们便规定由一个文字组成的排列是恒等排列.

容易证明，任意一个排列可以用没有公共文字的循环排列的乘积来表示，譬如

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (134)(25),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (123),$$

其中因子显然是可以相互交换的. 假如不计因子的顺序，那么这种表示就是唯一的，也就是说，任意一个排列可以唯一地表为没有公共文字循环排列的乘积. 又任意循环排列可以用对换的乘积来表示，但这种表示不是唯一的，并且与因子的顺序有关. 譬如

$$\begin{aligned}(123\cdots n) &= (12)(23)\cdots(n-1\ n) \\ &= (1\ n)(1\ n-1)\cdots(12),\end{aligned}$$

$$\begin{aligned}(25) &= (12)(15)(12) = (15)(12)(15) \\ &= (45)(34)(23)(34)(45).\end{aligned}$$

下面是排列用对换的乘积表示时一个重要的不变性质.

定理 3 假如一个排列用对换的乘积来表示，那么对换因子的个数是偶数或奇数是一定的，也就是说，是偶数时永远是偶数，是奇数时永远是奇数.

证明 假设 n 个文字 $a_1, \cdots, a_n$ 的函数

$$\begin{aligned}F = \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j) = {} & (a_{n-1} - a_n) \\ & \cdot (a_{n-2} - a_n)(a_{n-2} - a_{n-1}) \\ & \cdot \cdots \\ & \cdot (a_1 - a_n)(a_1 - a_{n-1}) \cdots (a_1 - a_2),\end{aligned}$$

我们把 F 写成

$$F = (a_k - a_l) \prod_{i \neq k, l} (a_i - a_k)(a_i - a_l) f,$$

这里 f 不包括 a_k 及 a_l. 现在 F 上施行对换 $(a_k a_l)$，我们容易知道 f

及$(a_i-a_k)(a_i-a_l)$都不变动，但a_k-a_l变了符号，所以F就换成为$-F$. 这就是说，在F上施行任一个对换，F就变符号，因此，在F上假如继续施行偶数个对换，结果仍然是F，假如继续施行奇数个对换，结果就是$-F$. 但是在F上施行一个排列的结果是一定的，因此一个排列不能同时表为偶数个对换的乘积，又表为奇数个对换的乘积，所以定理成立.

一个排列，它的对换因子的个数假如是偶数，就叫做**偶排列**，假如是奇数就叫做**奇排列**，一个偶排列与一个奇排列的乘积是奇排列，两个偶排列或两个奇排列的乘积都是偶排列. 恒等排列是偶排列[4]. 一个循环排列，它所含文字的个数如果是偶数就是奇排列，如果是奇数就是偶排列.

因为两个偶排列的乘积仍然是偶排列，所以在n个文字上的对称群S_n中所有偶排列成为一个子群，叫做n个文字上的**交代群**，用A_n来表示，它是S_n中一个非常重要的子群. 再对称群S_n中偶排列个数与奇排列个数相等. 这是因为用S_n中某一奇排列乘其中所有偶排列就得到互异的奇排列，因此S_n中偶排列不多于奇排列. 同样，S_n中奇排列又不多于偶排列，所以S_n中偶排列个数与奇排列个数相等. 因为$|S_n|=n!$，所以

$$|A_n|=\frac{n!}{2},$$

譬如，三个文字上的对称群

$$S_3=\{(1),(12),(13),(23),(123),(132)\},$$

4个文字上的交代群

$$A_4=\{(1),(12)(34),(13)(24),(14)(23),(123),$$
$$(124),(134),(234),(132),(142),(143),(243)\}.$$

下面是关于排列的一个简便算法，在具体计算时非常有用. 假如τ,σ是两个排列，如果把τ写成没有公共元的循环排列的乘积，并且循环排列中的文字用σ中所变换的文字来代替，那么得到的排列就是$\sigma\tau\sigma^{-1}$. 这是因为$\sigma\tau\sigma^{-1}(\sigma(a))=\sigma\tau(a)$即$\sigma(a)\to\sigma\tau(a)$，因

此如果 $\tau=(a_1a_2)(b_1b_2b_3)$，那么

$$\sigma\tau\sigma^{-1}=(\sigma(a_1)\sigma(a_2))(\sigma(b_1)\sigma(b_2)\sigma(b_3)).$$

譬如，$\tau=(314)(25)(67)$，$\sigma=(123)(567)$，那么

$$\sigma\tau\sigma^{-1}=(124)(36)(75).$$

最后来讨论循环群的子群，我们先介绍循环群.

由一个元 a 生成的群是由元 a 的所有乘幂 a^n 组成的，用 $\langle a\rangle$ 也常常用 (a) 表示，a 叫做**生成元**，这时

$$a^m\cdot a^n=a^{m+n},\ a^0=e,\ a^{-n}=(a^{-1})^n.$$

一个群如果是由其中一个元生成的就叫做**循环群**.

譬如 A_3 是元数是 3 的循环群，(123)，(132)都是它的生成元，即 $A_3=((123))=((132))$. 整数集 $\mathbf{Z}$ 对加法形成的加群是无穷循环群，1，-1 都是它的生成元，即 $\mathbf{Z}=(1)=(-1)$. 因此循环群的生成元不是唯一的.

循环群在群中构造是最简单的，并且也是最基本的. 下面，我们来讨论循环群 (a) 的构造.

假定 a 的所有乘幂都互不相等，即当 $h\neq k$ 时，$a^h\neq a^k$，因此这时循环群 (a) 是由下面的元组成的：

$$\cdots,a^{-2},a^{-1},a^0,a^1,a^2,\cdots,$$

它是无穷群.

假定 a 的乘幂中有相等的，并且 $h>k$ 时，$a^h=a^k$，这时我们有

$$a^{h-k}=e,\ h-k>0.$$

如果 n 是使 $a^n=e$ 成立的最小正整数，那么 $a^0,a^1,\cdots,a^{n-1}$ 彼此互异，这是因为假如 $a^i=a^j$，$0\leqslant j<i<n$，那么

$$a^{i-j}=e,\ 0<i-j<n.$$

这与 n 是最小正整数的假定矛盾. 再假如把任意整数 m 写成

$$m=qn+r,\ 0\leqslant r<n,$$

那就有

$$a^m=a^{qn+r}=a^{qn}\cdot a^r=(a^n)^q\cdot a^r=ea^r=a^r,$$

所以 a 的任意乘幂都与 $a^0,a^1,\cdots,a^{n-1}$ 中某一个相等，因此这时循

环群(a)只含有n个元：

$$a^0, a^1, \cdots, a^{n-1},$$

它是有穷群，元数是n.

假如a的任意两个乘幂都不相等，我们就说a的阶是无穷. 假如a的乘幂中有相等的，n是使$a^n=e$成立的最小正整数，我们就说a的阶数是n.

譬如，群的单位元的阶数是1，A_3的生成元(123)的阶数是3. 再在整数集$\mathbf{Z}$组成的加群中，任意非零的整数的阶都是无穷.

下面是阶数的一个基本性质：假如a的阶是无穷，那么当$a^m=e$时，$m=0$，因此$a^r=a^s$的必要充分条件是$r=s$. 假如a的阶数是n，那么，当$a^m=e$时，$m\equiv 0\ (n)$，也就是说，m是n的倍数，即$n|m$，这是因为m可以写成$m=qn+r$，$0\leqslant r<n$，于是

$$a^r=a^m\cdot a^{-qn}=a^m=e,$$

因为n是阶数，所以$r=0$，即$m=qn$，因此$a^r=a^s$的必要充分条件是$r\equiv s(n)$.

于是由上面的讨论，我们有

定理4 一个循环群(a)，假如a的阶是无穷，那么它是无穷群：

$$(a)=\{\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots\}.$$

假如a的阶数是n，那么它是元数等于n的有穷群：

$$(a)=\{a^0, a^1, \cdots, a^{n-1}\},\quad a^n=a^0.$$

现在来讨论循环群的子群.

假如G是由元a生成的循环群，即$G=(a)$，H是G的子群，但不是单位元群，也就是说，H不是只由单位元组成的，那么H中必含有幂$m>0$的元a^m. 这是因为，假如$m<0$，那么a^m的逆元a^{-m}也在H中，这时$-m>0$. 假设a^m是H中a的最小正幂，显然H包含a^m的任意乘幂. 假如a^s是H中任意元，由

$$s=tm+r,\quad 0\leqslant r<m,$$

我们得知

$$a^r = a^{s-tm} = a^s \cdot (a^m)^{-t}$$

也是 H 中元，但 m 是最小正整数，而 $0 \leqslant r < m$，因此 $r=0$，于是

$$a^s = (a^m)^t,$$

这就是说，H 中任意元是 a^m 的乘幂，也就是说 H 只含 a^m 的任意乘幂，所以 H 是由 a^m 生成的循环群，即 $H=(a^m)$. 因为 G 中任意元的 m 乘幂是 a^m 的乘幂，所以 H 又可以看成是由 G 中各元的 m 乘幂组成的子群.

假如 a 的阶是无穷，那么 a^m 的阶也是无穷，于是 H 是由下面无穷多个元形成的：

$$(a^m)^0 = e, a^{\pm m}, a^{\pm 2m}, \cdots,$$

所以这时它是无穷群.

假如 a 的阶数是 n，即 $a^n = e$. 因为 a^m 是 H 中 a 的最小正幂，而 $a^n \in H$，所以 n 能够用 m 整除，命 $n=qm$，那么 a^m 的阶数是 q，于是 H 只包含下面 q 个元：

$$a^0, a^m, a^{2m}, \cdots, a^{(q-1)m}.$$

所以这时 H 是元数为 q 的有穷群. G 中元数是 q 的子群显然只是由 a^m 生成的，因此 G 只有唯一一个 q 元子群.

由上面讨论的结果，我们有

定理 5 循环群 $G=(a)$ 的子群 H 还是循环群. 假如 H 不是单位元群，那它就是由其中元 a 的最小正幂 a^m 生成的，也就是说，H 是由 G 中所有各元的 m 乘幂组成的. 当 G 是无穷群时，H 也是无穷群. 当 G 的元数是 n 时，这 m 是 n 的约数，因此 H 的元数是 $q=\dfrac{n}{m}$，并且 H 是 G 中唯一一个 q 元子群.

于是，无穷循环群有无穷个子群，n 元循环群的子群的个数等于 n 中互异正因数的个数.

群 G 中所有各元的 m 乘幂组成的子集，我们用 G^m 表示，由上面定理，我们得知循环群 G 的子群是 G^m，m 是正整数.

1956 年石兹(F. Szász)证明了它的逆，即交换群 G，如果它的

子群都是G^m,m是正整数,那么G是循环群. 因此交换群G是循环群的必要充分条件是它的子群都是G^m(m是正整数)的形状[5].

假如G是非交换群,G^m不一定成群,譬如$S_3^3=\{(1),(12),(13),(23)\}$就不是$S_3$的子群. 假如$G$是交换群,对于任意正整数$m$,显然$G^m$都是$G$的子群. 其实,$m$是负整数时也同样成立. 当然$G$的子群不一定都是$G^m$的形状. 再假如对任意整数$m$,$G^m$都是群$G$的子群,$G$不一定是交换群,譬如四元数群(§2.3)就是一例.

要注意的是,循环群(a)中任意元a^m生成的群(a^m)当然都是(a)的子群,但a^m不一定就是(a^m)中a的最小正幂. 当(a)是无穷群时,a^m是(a^m)中a的最小正幂. 当(a)的元数是n时,只有$m|n$时,a^m才是(a^m)中a的最小正幂. 譬如$n=6$时,

$$(a^4)=(a^2),\quad (a^5)=(a).$$

循环群中两个子群相等与否,根据前面阶数的性质,我们容易有下面定理:

定理6 假定循环群(a)是无穷群,那么它的子群$(a^r)=(a^s)$的必要充分条件是$r=\pm s$.

证明 当$r=\pm s$时,显然$(a^r)=(a^s)$,因此充分条件成立. 反过来,假如$(a^r)=(a^s)$,那么$a^r=(a^s)^h=a^{sh}$,因此$r=sh$. 同样$s=rk$. 于是$s=skh$,即$kh=1$,但h,k都是整数,所以$h=k=\pm 1$,于是$r=\pm s$,因此必要条件成立. 证毕.

特别,当$s=1$时,我们即得:循环群(a),如果是无穷群,那么只有两个元a,a^{-1}可做它的生成元,即$(a)=(a^{-1})$.

定理7 假定(a)是n阶循环群,那么它的子群$(a^r)=(a^s)$的必要充分条件是r与n的最大公因数同s与n的最大公因数相等. 即$(r,n)=(s,n)$.

证明 假如$(a^r)=(a^s)$,因为$a^r=(a^s)^h=a^{sh}$,所以$r\equiv sh(n)$. 即$r=sh+nk$,所以$(s,n)|r$,因此$(s,n)|(r,n)$. 同样我们又有$(r,n)|s$因此$(r,n)|(s,n)$所以$(r,n)=(s,n)$. 反过来,假如$(r,n)=(s,n)$,那么$(s,n)|r$,因此不定方程$r=sh+nk$有解,即有满足该式

的整数 h,k. 于是 $a^r\in(a^s)$. 同样,我们又有 $a^s\in(a^r)$,所以

$$(a^r)=(a^s).$$

定理证毕.

特别假如 $s=1$,那么 $(a^r)=(a)$ 的必要充分条件是 $(r,n)=1$,这就是说 n 阶循环群 (a) 只有对与 n 互质的正整数 r 的 a^r 做它的生成元,小于 n 且与 n 互质的正整数的个数欧拉(L. Euler,1707—1783)用 $\varphi(n)$ 表示,叫做**欧拉函数**. 因此 (a) 有 $\varphi(n)$ 个生成元.

譬如,n 次单位根也就是 n 次多项式 x^n-1 的零点

$$\xi_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\quad k=1,\cdots,n$$

组成 n 元循环群,它的生成元是 ξ_r,这里 $(r,n)=1$. 因此元数是任意自然数的循环群是存在的.

一个群究竟有多少个子群? 子群的构造如何?

这是群论中主要问题之一. 在一般情况下,这问题还没有得到解决. 由定理 4 及定理 5,我们得知对于循环群来说这问题算是解决了的. 密勒尔(G. A. Miller)曾由子群的个数及性质来讨论群的构造,得到了不少的好结果[6],这里当然都不能谈了.

上面是讨论循环群,下面我们介绍由若干个元生成的群.

假定 M 是群 G 的子集,当然它不一定成群,因为 M 中任意两元的积以及任意元的逆虽然都在 G 中,但不一定都在 M 中. 如果我们把这样的一些积以及逆都添加于 M,那它就成为子群. 这子群包含 M,叫做由 M **生成的群**,用 $\langle M\rangle$ 来表示,这时我们又说 M 是 $\langle M\rangle$ 的**生成元集**,M 中元又叫做 $\langle M\rangle$ 的**生成元**. 因为我们的添加只是添加 M 中元的积及逆,当添加一旦成群后,就不再添加,所以 $\langle M\rangle$ 是 G 中包含 M 的最小子群,或者说 $\langle M\rangle$ 是 G 中所有包含 M 的子群的交集. 当 M 自身是子群时,$\langle M\rangle=M$.

譬如,由 $(1234),(12)(34)$ 生成的群

$$D_8=\langle(1234),(12)(34)\rangle=\{(1),(1,3),(2,4),$$
$$(12)(34),(13)(24),(14)(23),(1432),(1234)\}$$

假如命 $a=(1234)$，$b=(12)(34)$，可简写成

$$D_8=\langle a,b\rangle,\ a^4=1,\ b^2=1,\ ab=ba^3.$$

它是 8 元群，叫做二面体群，是一个常见的群.

假如 $M=\{a_1,a_2,\cdots,a_n\}$，那么 $\langle M\rangle$ 中任意元可以表为

$$a_{i_1}{}^{m_1}a_{i_2}{}^{m_2}\cdots a_{i_r}{}^{m_r},$$

这里 $a_{i_j}\in M$，m_j 是正负整数或零，$a_{i_1},a_{i_2},\cdots,a_{i_r}$ 中相邻的不相等，不相邻的可能相等，假如 M 中任意两元 a_i,a_j 都能够交换，即 $a_ia_j=a_ja_i$，那么 $\langle M\rangle$ 中任意元的形状是

$$a_1{}^{m_1}a_2{}^{m_2}\cdots a_n{}^{m_n}$$

这里 m_i 是正、负整数或零.

上面介绍由 M 生成的群，其中 M 是群的子集，下面我们介绍由任意集合生成的群.

假定 $X=\{x_i|i\in I\}$ 是非空集合不一定是有穷或可数. 我们把与记号 x_i 一一对应的新记号记成 x_i^{-1}，令 $X^{-1}=\{x_i^{-1}|i\in I\}$，$x_i$ 有时又写成 x_i^{+1}，在 X 或 X^{-1} 中取有穷个记号作成的表达式

(1) $$w=x_{i_1}{}^{w_1}x_{i_2}{}^{w_2}\cdots x_{i_n}{}^{w_n},\quad w_i=\pm1$$

叫做 X 上的一个字. 在(1)中规定 x_i^1 与 x_i^{-1} 不相邻，或者说它们相邻时可以相互抵消而不出现. 譬如 $x_1x_2^{-1}x_2x_3$ 可以缩写成 x_1x_3. 再为了简便相同的可以用幂的形式表出，譬如 $x_1x_2x_2$ 或 $x_1^{-1}x_1^{-1}x_3$ 可以简写成 $x_1x_2^2$ 或 $x_1^{-2}x_3$. 我们也把不含记号的字叫做空字用 w_0 表示. 两个字

$$w_1=x_{i_1}{}^{m_1}x_{i_2}{}^{m_2}\cdots x_{i_k}{}^{m_k},\quad w_2=x_{j_1}{}^{n_1}x_{j_2}{}^{n_2}\cdots x_{j_l}{}^{n_l}$$

的乘积 w_1w_2 我们规定是把 w_1,w_2 的表达式连写，即

$$w_1w_2=x_{i_1}{}^{m_1}x_{i_2}{}^{m_2}\cdots x_{i_k}{}^{m_k}x_{j_1}{}^{n_1}x_{j_2}{}^{n_2}\cdots x_{j_l}{}^{n_l},$$

其中如果有 x_i 与 x_i^{-1} 相邻的即进行缩写. 显然 X 上任意两个字的乘积仍然是 X 上的一个字. 空字 w_0 在乘法中起单位元的作用. 容易知道

$$w_1^{-1}=x_{i_k}^{-m_k}\cdots x_{i_2}^{-m_2}x_{i_1}^{-m_1}$$

是 w_1 的逆. 再乘法的结合律 $w_1(w_2w_3)=(w_1w_2)w_3$ 用归纳法也不难证明. 因此由 X 上的字组成一个群叫做由 X 生成的自由群，它不依赖 X 中记号的个别性质. X 所含记号的个数叫做该自由群的秩.

显然秩是 1 的自由群是无穷循环群. 任意秩大于 2 的自由群都不是交换群.

习　题　2.2

1. 试证下列各式：

(i) $(12)(34)(15)(23)(45)=(153)(24)$;

(ii) $(1ij)=(12j)^2(12i)(12j)$;

(iii) $(ac)(bd)=(abd)(acd)$.

2. 试求循环加群 $\mathbf{Z}-(100)$的所有子群.

3. 假定元 a 的阶数是 n，试证 a^m 的阶数是 $\frac{n}{(n,m)}$.

4. 假定 a,b 是群中元，$ab=ba$，元 a 的阶数是 m，元 b 的阶数是 n，那么它们的乘积 ab 的阶数是 m,n 的最小公倍数 q 的约数，并且群中含有阶数是 q 的元，当 m,n 互质时，ab 的阶数是 mn.

5. 假如交换群 G 中元的最大阶数是 m，试证：G 中任意元的阶数都是 m 的因数.

6. 在线性群 $GL(2,\mathbf{Z})$中

$$A=\begin{pmatrix}1 & 2\\ 0 & -1\end{pmatrix},\quad B=\begin{pmatrix}1 & 3\\ 0 & -1\end{pmatrix}$$

的阶数都是 2，试证：AB 的阶是无穷.

7. 写出 4 个文字上的交代群 A_4 的群表.

8. 证明：S_n 可以用 $n-1$ 个对换$(12),(13),\cdots,(1n)$ $(n>1)$生成.

9. 证明：A_n 可以用 $n-2$ 个 3 项循环排列$(123),(124),\cdots,(12n)$生成.

10. 假定 A,B 是群 G 的子群，那么 A,B 的并集 $A\cup B$ 是 G 的子群的必要充分条件是 $A\subseteq B$ 或 $B\subseteq A$.

11. 假定 G 是 n 元群，试证：n 是奇数的必要充分条件是 G 中除单位元外任意元可以写成另一元的平方.

§2.3 正 规 子 群

在§1.2中我们曾经把整数加群 **Z** 用子群(n)来分类，现在我们把它推广，来讨论一般群用它的子群来分类.

我们先介绍子集乘积的概念.

假设H,K是群G的两个子集，h是H中任意元，k是K中任意元，那么所有形如hk的元集，叫做H与K的乘积，或简称H，K的积，用记号HK表示，即

$$HK=\{hk\mid h\in H,k\in K\}$$

譬如，$H=\{(1),(12),(123)\}$，$K=\{(123),(132)\}$，那么

$$HK=\{(1),(13),(23),(132),(123)\}.$$

关于群中三个子集的乘积我们有

$$H(KL)=(HK)L.$$

这就是说，群中子集的乘积是满足结合律的. 当H是子群时，我们又有

$$HH=H.$$

要注意，它的逆不成立，即当$HH=H$时，H不一定成群. 譬如在整数加群 **Z** 中，正整数集并不成群.

对于有穷子群的乘积我们有

定理1 假定H,K是群G的有穷子群，那么

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}.$$

证明 假定$h_1k_1=h_2k_2$，$h_i\in H$，$k_i\in K$，那么

$$h_2^{-1}h_1=k_2k_1^{-1}=d\in H\cap K,$$

因此

$$h_2=h_1d^{-1},\ k_2=dk_1.$$

反过来，对于h_1,k_1，任取$H\cap K$中元d，设$h_2=h_1d^{-1}$，$k_2=dk_1$，就得到$h_1k_1=h_2k_2$，这就是说，对于任意h_1,k_1，在HK中有$|H\cap K|$

个与 h_1k_1 相等的元. 于是定理成立.

特别地当 $H\cap K=e$, 即 $|H\cap K|=1$ 时, $|HK|=|H|\cdot|K|$.

假定 H,K 都是 G 的子群, H,K 的乘积 HK 一般不一定成群. 但是在什么条件下, HK 也能成为群?

假如 HK 成群, h,k 分别是 H,K 中任意元, 因为 KH 中元 kh 是 HK 中元 $h^{-1}k^{-1}$的逆, 所以 $kh\in HK$, 因此 $KH\subseteq HK$. 又因为$(hk)^{-1}\in HK$, 命$(hk)^{-1}=h'k'$, 于是 $hk=k'^{-1}h'^{-1}\in KH$, 所以 $HK\subseteq KH$. 因此 $HK=KH$, 也就是说, 假如 HK 成群, 那么 H 与 K 能够交换.

反过来, 假如 $HK=KH$, 也就是说, H 与 K 能够交换, 那么 HK 中任意元 hk 的逆元 $k^{-1}h^{-1}$在 $KH=HK$ 中. 又因为

$$HKHK=HHKK=HK,$$

所以 HK 中任意两元的乘积仍然在 HK 中, 于是 HK 成群. 因此我们有下面的

定理 2 群 G 的子群 H,K 的乘积 HK 成群的必要充分条件是 H 与 K 能够交换.

要注意的是, 这里说的 H 与 K 能够交换, $HK=KH$, 是表示 $HK\subseteq KH$, 并且 $KH\subseteq HK$. 因此, 对于 H,K 中任意元 h,k, 我们不一定就能有 $hk=kh$, 一般只能有 $hk=k'h'$, $kh=h''k''$, 这里 h', h''; k', k''分别是 H,K 中元. 当 G 是交换群时, 显然 $HK=KH$. 所以交换群的任意两个子群的乘积仍然是一个子群.

由 § 2.2, 我们知道 HK 包含在由 H,K 生成的群$\langle H,K\rangle$中, 当 HK 成群时, 由 H,K 生成的群就是 HK, 即$\langle H,K\rangle=HK$, 也就是说, HK 是 G 中包含 H,K 的最小子群.

假如 G 是加群, 只要 H,K 是子群, 当然 HK 也是子群, 这时仍然把 HK 写成(H,K), 叫做 H,K 的和, 我们不用 $H+K$ 来表示, 因为后面(§ 6.4)要用它来表示直和.

特别地当 H 只包含一个元 h 时, H 与 K 的乘积 HK 就简单地写成 hK.

定义 1　假如 H 是 G 的子群，a 是 G 中任意元，那么集合 aH (Ha)，叫做 G 中 H 的左(右)陪集.

譬如 $G=S_3$，$H=\{(1),(12)\}$，那么 H 的左陪集

$$(13)H=\{(13),(123)\},\quad (23)H=\{(23),(132)\};$$

H 的右陪集

$$H(13)=\{(13),(132)\},\quad H(23)=\{(23),(123)\}.$$

因此，一个群的子群的左陪集不一定与它的右陪集一致. 当群是交换群时，陪集就无所谓左、右的了.

假如 a 在 H 中，那么 $aH=H$，这就是说，H 自身也是一个左陪集. 假如 $b\in aH$，那么 $aH=bH$，这就是说，左陪集 aH 由其中任一元唯一确定. 假如 a,b 在 H 的同一左陪集中，那么 $b=ah$，因此 $a^{-1}b=h\in H$. 反过来，假如 $a^{-1}b\in H$，那么 $b=ah$，$h\in H$，因此 a,b 在 H 的同一左陪集中. 于是 a,b 在 H 的同一左陪集中的必要充分条件是 $a^{-1}b\in H$.

假如 aH 成群，那么 $ah=e$，$h\in H$，所以 $a\in H$，因此 $aH=H$，这就是说，H 的陪集中只有 H 成群，其余都不成群.

假如把 aH 的元 ah 与 bH 的元 bh 相对应，我们就得到 aH 射到 bH 上的单射，因此两个左陪集 aH，bH 的浓度相等.

现在我们来讨论群 G 用它的子群 H 的陪集来分类.

因为 G 中任意元 a 必出现在 H 的左陪集 aH 中. 假如左陪集 aH，bH 有公共元 $ah=bh'$，那么 $a^{-1}b=hh'^{-1}\in H$，因此 $aH=bH$. 这就是说，G 中 H 的任意两个左陪集或者重合或者没有公共元. 于是，G 可以分解为若干个互异的左陪集 a_iH，$i=1,2,\cdots$，即

$$G=a_1H\cup a_2H\cup\cdots.$$

显然除陪集 a_iH 的顺序外，这分解是唯一的，但 a_i 不是唯一的.

同样，我们可以把 G 唯一地分解为若干个互异的右陪集 Hb_i，$i=1,2,\cdots$，即

$$G=Hb_1\cup Hb_2\cup\cdots.$$

用同一个子群把群分解为左陪集与分解为右陪集，其结果一

般是不一致的. 譬如交代群 A_4 对于克莱茵(F. Klein, 1849—1925)四元群

$$B_4=\{(1),(12)(34),(13)(24),(14)(23)\}$$

的左陪集分解与右陪集分解分别为

$$\begin{aligned} A_4 &= B_4 \cup (234)B_4 \cup (243)B_4 \\ &= B_4 \cup B_4(234) \cup B_4(243). \end{aligned}$$

又对称群 S_3 对于 $H=\{(1),(12)\}$ 的两种分解为

$$S_3=H\cup(13)H\cup(23)H=H\cup H(13)\cup H(23).$$

但 $(234)B_4=B_4(234)$, $(243)B_4=B_4(243)$, 而 $(13)H\neq H(13)$, $(23)H\neq H(23)$. 所以 A_4 对于 B_4 的两种分解是一致的, 而 S_3 对于 H 的两种分解不是一致的. 下面是左、右两种分解的一个重要关系.

定理 3 假设 H 是群 G 的子群, 并且

$$G=a_1H\cup a_2H\cup\cdots\cup a_nH\cup\cdots,$$

那么 $G=Ha_1^{-1}\cup Ha_2^{-1}\cup\cdots\cup Ha_n^{-1}\cup\cdots$.

证明 我们只要证明 G 中任意元 g 在某个右陪集 Ha_i^{-1} 中, 并且任意两个右陪集 Ha_i^{-1}, Ha_j^{-1} 都不相等就行了.

首先因为 $g\in G$, 所以 $g^{-1}\in G$. 因此 g^{-1} 在某一左陪集 a_iH 中, 即 $g^{-1}=a_ih$, 于是 $g=h^{-1}a_i^{-1}\in Ha_i^{-1}$.

再如果 $Ha_i^{-1}=Ha_j^{-1}$, 那么 $a_i^{-1}a_j\in H$, 因此 $a_iH=a_jH$, 这与假设不合, 所以 Ha_i^{-1}, Ha_j^{-1} 是相异的右陪集, 因此定理得证.

因为集合 $\{a_1,a_2,\cdots,a_n,\cdots\}$ 与集合 $\{a_1^{-1},a_2^{-1},\cdots,a_n^{-1},\cdots\}$ 显然有相等的浓度, 所以 G 中 H 的相异左陪集的个数(即浓度), 与相异右陪集的个数一致. 这样我们有

定义 2 群 G 中子群 H 的相异左(右)陪集的个数, 叫做 H 在 G 的**指标**, 用记号 $|G:H|$ 表示.

因为对左陪集能够成立的性质, 对右陪集来说也能够同样证明, 所以后面我们讨论陪集时, 只就左陪集而言.

指标可以是有穷也可以是无穷. 譬如从 §1.2, $|\mathbf{Z}:(n)|=n$,

又$|A_4:B_4|=3$，$|S_3:H|=3$. 再假如G是所有有理数对加法组成的加群，H是所有整数组成的子群，那么$|G:H|$是无穷，这是因为

$$1,\ \frac{1}{2},\ \cdots,\ \frac{1}{2^n},\ \cdots$$

显然分别在H的不同陪集$\frac{1}{2^i}+H$，$i=0,1,\cdots$中.

假如G是有穷群，H是子群，那么

$$|G|=|H|\cdot|G:H|,$$

这是因为G有$|G:H|$个互异的左陪集，并且每个左陪集又都有$|H|$个元. 于是我们得下面的**拉格朗日**(J. Lagrange，1736—1813)**定理**.

定理 4 有穷群的子群的元数是这群的元数的因数.

由这定理，我们容易得知当p是质数时，p元群没有异于单位元群的真子群. p^n元循环群只有n个真子群. 1939年密勒尔曾证明，含12个真子群的群只有元数是p^{12}的循环群[7]. 一般元数是质数p的幂的群叫做**p-群**.

定理4是有穷群的一个重要性质，在很多地方我们将要引用它. 特别因为由一个元生成的循环群的元数就是这元的阶数，因此，一个元的阶数是这群的元数的因数. 于是，对于n元群中任意元a，阶数是n的约数，并且

$$a^n=e.$$

拉格朗日定理的逆对于循环群显然成立，就是对于交换群也是成立的(§6.5)，但一般不成立. 这就是说，假定G的元数是n，如果$m|n$，那么G不一定有m元子群. 譬如，交代群A_4是12元群，它就没有6元子群，但也有满足这逆的群[8]. 假如m再满足某些条件，这逆定理还是能成立的. 这问题的主要结果是西洛(L. Sylow，1832—1918)给出的，我们把这些结果概括为两个定理. 下面是著名的**西洛第一定理**.

定理 5 假定有穷群G的元数是n，p是质数，并且$p^r|n$，那么

G 有 p^r 元子群，当 r 是最大的幂指数时，这 p^r 元子群，叫做 G 属于 p 的西洛子群，或简称 p 西洛子群.

这样西洛第一定理就是说假如质数 $p \mid |G|$，那么 G 的 p 西洛子群是存在的.

譬如 A_4 的元数是 $12=2^2 \cdot 3$，那么它的 2 西洛子群是 B_4，它的 3 西洛子群是由(123)，(134)，(142)，(234)生成的 4 个 3 元循环群.

在这里我们只把定理提出，至于证明，因为需要另外的性质，把它放在§2.4 中.

假定群 G 的元数是 n，质数 $p \mid n$，由上述定理，G 中有元数为 p^r 的子群 H，因此 H 中有阶为 p 的元，这就是下面的柯西(A. L. Cauchy，1789—1857)定理.

定理 6 假定质数 p 能够整除群 G 的元数，那么 G 中有阶为 p 的元.

假如 G 是 p 群，即 $|G|=p^m$，由定理 4 知 G 中任意元的阶数是 p 的幂. 反过来，假如 n 元群 G 中任意元的阶数都是质数 p 的幂，那么 n 也是 p 的幂，因此 G 是 p 群. 这是因为假如 $q \mid n$，$(p,q)=1$，由定理 5，G 有 q 元子群，但其中任意元的阶数是 p 的幂，这显然与定理 4 矛盾，于是我们有

定理 7 有穷群是 p 群的必要充分条件是其中任意元的阶数都是 p 的幂.

上面主要介绍陪集. 下面，我们引用陪集介绍正规子群的定义并给出一些基本性质，在下两节及第 6 章中，我们将看到在群的另一些基本性质中，正规子群是非常重要的子群，在讨论群时，几乎处处都需要它.

一般 H 的左陪集不一定又是右陪集. 假如 H 的一个左陪集同时又是 H 的右陪集，那么对于这陪集中任意元 a，我们有 $aH=Ha$，也就是说 a 与 H 能够交换.

定义 3 假如群 G 中子群 H 的任意左陪集同时又是 H 的右

陪集，也就是说，H 能够与 G 中任意元 a 交换，即

(1) $$aH=Ha,$$

那么 H 叫做 G 的**正规子群**. 用 $H\lhd G$ 表示.

譬如，对称群 S_3 的子群$\{(1),(123),(132)\}$是它的正规子群，而子群$\{(1),(12)\}$，$\{(1),(13)\}$，$\{(1),(23)\}$都不是它的正规子群. 群 G 自身及单位元群显然都是 G 的正规子群.

上面(1)式可以改写成不等式

$$aHa^{-1}\subseteq H,\ a\in G.$$

再因为上面不等式对于 G 中任意元 a 都成立，当然对于 a^{-1} 也同样成立，因此 $a^{-1}Ha\subseteq H$，即 $H\subseteq aHa^{-1}$，所以 $aHa^{-1}=H$，也就是 $aH=Ha$，这就是说，(1)式可以用上面不等式来代替. 因此 G 的子群 H，如果包含元 h，且它也包含所有的 aha^{-1}，$a\in G$，那么 $H\lhd G$.

假定 A，B 分别是线性群 $GL(n,K)$ 及特殊线性群 $SL(n,K)$ 中任意元，我们容易得知 ABA^{-1} 的行列式是 1，所以 $ABA^{-1}\in SL(n,K)$，因此 $SL(n,K)\lhd GL(n,K)$.

我们知道，奇排列的逆是奇排列，偶排列的逆是偶排列，因此对于对称群 S_n 中任意排列 s，显然 sA_ns^{-1} 的排列都是偶排列，所以 $sA_ns^{-1}\subseteq A_n$，于是 $A_n\lhd S_n$.

我们容易证明，群 G 中所有与 G 中任意元能够交换的元成为一个正规子群，这是 G 的一个重要正规子群，叫做 G 的**中心**，用 $Z(G)$ 表示. 假如 G 是交换群，那么 G 的中心就是它自身. 当 G 的中心是单位元群时，有时又说 G **没有中心**. 譬如由(12)，(14)(23)生成的群$\langle(12),(14)(23)\rangle$的中心是$\{(1),(12)(34)\}$；$S_3$，$A_4$ 的中心都是单位元群，因此 S_3，A_4 都没有中心.

我们知道，交换群的子群都是正规子群，但它的逆不成立，也有这样的非交换群存在，它的任意子群都是正规子群，这类非交换群叫做**汉弥尔顿**(W. R. Hamilton，1805—1865)**群**[10].

我们知道，假如 H，K 都是群 G 的子群，并且 $G\supseteq K\supseteq H$，如果 H 是 G 的正规子群，由定义容易得知，H 也是 K 的正规子群. 但

要注意，K 不一定是 G 的正规子群. 再假如 H 是 K 的正规子群，K 是 G 的正规子群，但 H 不一定就是 G 的正规子群. 这就是说，正规子群这个关系是不适合传递律的. 譬如，克莱茵四元群 B_4 是对称群 S_4 的正规子群，因为 B_4 是交换群，所以 $\{(1),(12),(34),(12)(34)\}$ 是 B_4 的正规子群，但它不是 S_4 的正规子群.

由定义我们容易得知，在同一个群中，两个子群的乘积不一定成群，一个子群与一个正规子群的乘积是一个子群，两个正规子群的乘积是一个正规子群. 再两个子群的交是一个子群，一个子群与一个正规子群的交还是子群，两个正规子群的交是正规子群.

再由定义得知，假如 G 的子群 H 是正规子群，那么 G 中任意元与 H 能够交换. 假如 H 不是正规子群，那么 G 中有与 H 不能够交换的元. 一般 G 中所有与它的子集 H 能够交换的元成为子群，叫做 G 中 H 的**正规化子**. 用 $N(H)$ 表示，即

$$N(H)=\{x \mid x\in G, xH=Hx\}.$$

譬如，交代群 A_4 的子群 $\{(1),(234),(243)\}$ 的正规化子就是子群自身. 显然 H 是 $N(H)$ 的正规子群，并且 $H\subseteq N(H)\subseteq G$. $N(H)=G$ 的必要充分条件是 $H\lhd G$.

一个群至少有两个正规子群，一个是它自身，一个是单位元群. 只有这两个正规子群的群，就叫做**单纯群**，或简称**单群**. 显然，单位元群是单群，元数是质数的群也是单群. 再因为拉格朗日定理的逆对于交换群成立（在 § 6.5 中有证明）我们容易得知交换群只在元数为 1 或者是质数时，才是单群. 交代群 $A_n(n>4)$ 是一个重要的单群[11].

至于非交换群，元数不大于 1000 的只有元数是

$$60,\ 168,\ 360,\ 504,\ 660$$

的 5 个是单群. 1901 年狄克生（L. E. Dickson，1874—1954）曾揭示元数不大于百万的单群只有 53 个[11]. 这 53 个单群，它们的元数都是偶数. 伯恩赛德（W. Burnside，1852—1927）认为非交换单群的元数都是偶数，这是群论中长期没有得到证明的问题，1963 年

已由怀特(W. Feit)及汤卜生(J. G. Thompson)予以证实[12].

下面,我们证明用正规子群分类得到的陪集能够形成为群,这是一类由正规子群决定的重要群.

假如 H 是 G 的正规子群,那么 G 中元 a 所在的左陪集 aH 与元 b 所在的左陪集 bH 的乘积

$$aH\cdot bH=aHb\cdot H=ab\cdot HH=abH.$$

如果我们把 a 所在的左陪集 aH 用 $\bar{a}$ 表示,那就有

$$\bar{a}\cdot\bar{b}=\overline{ab}.$$

因此 G 中所有 H 的左陪集成为一个乘集.再我们容易知道,H 自身是这乘集的单位元,$\overline{a^{-1}}$是 $\bar{a}$ 的逆元,即 $\bar{a}^{-1}=\overline{a^{-1}}$.又因为 G 中元 a,b,c 满足结合律,所以左陪集 $\bar{a},\bar{b},\bar{c}$ 也满足结合律.因此把 H 的左陪集看成为元素时,所有这些左陪集形成为群,叫做 G 关于 H 的**商群**,用 G/H 表示.它的元数显然是 $|G:H|$.

当 G 是加群时,G 中 H 的陪集又叫做 H 的**同余类**,因此,H 的商群又叫做**同余群**,因为它是加群,所以又常常叫做**同余加群**,有时又叫做**差群**,用 $G-H$ 表示*).假如 G 是加群,H 是它的子群,如果 G 中元 a,b 同在 H 的一个同余类中,那么它们的差 $a-b\in H$,我们用**同余式**

$$a\equiv b\ (\mathrm{mod}\ H)\quad 或\quad a\equiv b\ (H)$$

表示,这时 a,b 又叫做关于 H **是同余的**.当 $a\equiv 0\ (H)$时,a 属于 0 所在的同余类,因此 $a\in H$.假如 $H=(h)$,我们又常常把 $a\equiv b(H)$ 写成 $a\equiv b\ (h)$,因此§1.2 所用的记号就是这里的特例.

譬如,整数加群 $\mathbf{Z}$ 关于(n)的同余加群

$$\bar{\mathbf{Z}}_n=\mathbf{Z}-(n)=\{\bar{0},\bar{1},\cdots,\overline{n-1}\},$$

它的元数是 n,结合法是 $\bar{a}+\bar{b}=\overline{a+b}$,也就是当 $a+b\equiv c\ (n)$时,

$$\bar{a}+\bar{b}=\bar{c}.$$

我们知道,有穷群中任意元的阶数都是有穷的,但反过来不一

*) 有的书或文献中仍用 G/H 表示.

定成立. 一个群如果其中任意元的阶数都是有穷的,叫做**周期群**或**扭群**,如果除单位元外任意元的阶数都是无穷时,叫做**纯无穷群**或**无扭群**,譬如,有穷群是周期群,无穷循环群是纯无穷群.

定理 8 假定 G 是交换群,H 是 G 中所有阶数是有穷的元集合,那么 H 是周期群,并且 G/H 是纯无穷群.

证明 假定 $a^m=e, b^n=e$,那么

$$(ab^{-1})^{mn}=a^{mn}(b^{mn})^{-1}=e,$$

所以 H 成群,因此 H 是周期群. 再假如 $\bar{a}$ 是 $\bar{G}=G/H$ 中任意元,如果 $\bar{a}^m=\overline{a^m}=\bar{e}$,那么 $a^m\in H$,因此 $(a^m)^n=a^{mn}=e$,于是 $a\in H$,所以 $\bar{a}=\bar{e}$,即 $\bar{G}$ 中阶数是有穷的元只有单位元,因此 $\bar{G}$ 是纯无穷群. 定理证毕.

我们知道,交换群的商群当然还是交换群,但它的逆并不成立,也就是说,有时非交换群的商群也是交换群. 最后我们介绍一个具有这性质的重要正规子群来结束本节.

假定 a,b 是群 G 中任意元,如果 $ab=ba$,那么 $a^{-1}b^{-1}ab=e$,如果 $ab\neq ba$,命

$$[a,b]=a^{-1}b^{-1}ab, \quad 即\ ab=ba\cdot[a,b],$$

这就是说,ba 用 $[a,b]$ 右乘后就变为 ab 了,因此我们叫 $[a,b]$ 做 a,b 的**换位子**. 显然 a,b 的换位子是 b,a 换位子的逆. 当 G 是交换群时,只有单位元是它的换位子. 反过来,一个群的换位子如果只是单位元,显然这群是交换群. 一个群的两个换位子的乘积一般不再是这群的换位子[13]. 因此,一个群的所有换位子不一定能成为群. 我们把 G 中所有换位子生成的群叫做 G 的**换位子群**,用 $D(G)$ 或 G' 来表示. 因此群 G 是交换群的必要充分条件是 $D(G)$ 是单位元群.

假定 G' 是 G 的换位子群,a,g 分别是 G,G' 中任意元,因为 g 也是 G 中元,由 $aga^{-1}g^{-1}\in G'$,我们有

$$aga^{-1}=aga^{-1}g^{-1}\cdot g\in G',$$

因此 $aG'a^{-1}\subseteq G'$,所以 G' 是 G 的正规子群. 再由 $a^{-1}b^{-1}ab=g$,我

们有 $ab=bag$，于是$\overline{ab}=\overline{ba}$，即$\bar{a}\,\bar{b}=\bar{b}\,\bar{a}$，因此商群 G/G' 是交换群.

又假如 G/H 是交换群，由 $\bar{a}\,\bar{b}=\bar{b}\,\bar{a}$，我们就有 $ab=bah$，$h\in H$，因此 $a^{-1}b^{-1}ab\in H$，这就是说，H 包含 G'. 反过来，假如 H 是包含 G' 的正规子群，那么 G/H 是交换群，于是我们有

定理 9 群 G 的换位子群 G' 是 G 的正规子群，并且商群 G/G' 是交换群. G/H 是交换群的必要充分条件是 H 包含 G 的换位子群 G'.

于是群 G 的换位子群是使 G 的商群为交换群的最小正规子群. 假如 H 是群 G 的子群，如果 $H\supseteq G'$，那么 H 是 G 的正规子群，即包含 G' 的子群是正规子群，这是因为

$$ghg^{-1}=(ghg^{-1}h^{-1})h\in G'H\subseteq H.$$

我们容易知道 S_n/A_n 是交换群，所以 $D(S_n)\subseteq A_n$，再由§2.2习题 9，A_n，$n\geqslant 3$，是所有 3 项循环排列$(12i)$生成的群，但任意 3 项排列

$$(12i)=(21)^{-1}(i1)^{-1}(21)(i1),$$

即$(12i)$是 S_n 的换位子，因此 $A_n\subseteq D(S_n)$. 所以 $D(S_n)=A_n$. 又当 $n\geqslant 5$ 时，

$$(1a2)^{-1}(1bi)^{-1}(1a2)(1bi)$$
$$=(12a)(1ib)(1a2)(1bi)=(12i),$$

即$(12i)$是 A_n 的换位子，因此 $D(A_n)=A_n$，于是我们有

定理 10 对称群 S_n 的换位子群是交代群 A_n. 当 $n\geqslant 5$ 时，A_n 的换位子群是 A_n 自身.

习 题 2.3

1. 试证：元数是质数的群是循环群.
2. 试证：指标是 2 的子群是正规子群.
3. 假定 H 是 G 的子群，K 是 H 的子群，求证：
$$|G:K|=|G:H|\cdot|H:K|.$$
4. 假定 G 是循环群，H 是指标为 m 的子群，那么 G/H 是元数为 m 的循环群. 因此任意循环群 G 的子群 H 在 G 的指标$|G:H|$是有穷的.

5. 群G中子群H是正规子群的必要充分条件是:H的任意两个左陪集的乘积仍然是H的一个左陪集,如何证明?

6. 假定H,K是群G的正规子群,$H\cap K=E$,那么$hk=kh$,这里$h\in H$,$k\in K$.

7. 假定a,b,c是群中元,试证下列两式:

$$[ab,c]=[a,c][b,c],\ [a,bc]=[a,c][a,b].$$

8. 具有关系$i^2=j^2=k^2=-1,(-1)^2=1$,

$$ij=k=-ji,\ jk=i=-kj,\ ki=j=-ik$$

的数i,j,k是基本四元数(§3.2),因此,由$\pm i,\pm j,\pm k,\pm 1$八个数组成的8元群,叫做**四元数群**.试证:四元数群的2元子群只有(-1)一个,4元子群有$(i),(j),(k)$三个,它们都是正规子群.于是四元群是汉弥尔顿群.

9. 试证:四元数群可以写成

$$\langle a,b\rangle,\ a^4=1,\ b^2=a^2,\ ab=ba^3.$$

10. 假如G是四元数群,试证:对于任意正整数m,G^m是G的子群.

11. 试求交代群A_4的子群,并指出何者是正规子群.

12. 试证:交代群A_3的换位子群是单位元群,A_4的换位子群是克莱茵四元群B_4.

13. 试证:对称群S_n,$n\geqslant 3$的中心是单位元群.

14. 试证:对称群S_4的正规子群除自身及单位元群外,只有交代群A_4及克莱茵四元群B_4.

15. 假如已知$n>4$时交代群A_n是单群,试证:$n\neq 4$时,对称群S_n除自身及单位元群外,只有A_n是它的唯一正规子群.

§2.4 同 构

映射这个概念,对于代数系必须与结合法或代数运算发生联系,才能成为有力工具.因此在讨论代数系时,我们需要的是与结合法相适应的映射.显然,两元的乘积的像等于这两元的像的乘积是一个重要联系,此后两节就是讨论具有这联系的重要映射.

定义 假设M,M'是两个乘集,也就是说,M,M'是两个各具有一个闭合的结合法(写成乘法)的代数系,σ是M射到M'的双

射，并且任意两元的乘积的像是这两元的像的乘积，即对于 M 中任意两元 a,b，

$$\sigma(a\cdot b)=\sigma(a)\cdot\sigma(b),$$

也就是说，当 $a\to\sigma(a)$，$b\to\sigma(b)$ 时，$ab\to\sigma(a)\sigma(b)$，那么这映射 σ 就叫做 M 到 M' **上的同构**. 我们又叫 M 与 M' **同构**，用 $M\simeq M'$ 表示.

因为双射是等价关系，所以同构这个关系也是等价关系.

譬如，结合法都是乘法的两个群

$$G=\{1,i,-1,-i\},\quad G'=\{\sigma_0,\sigma_{90},\sigma_{180},\sigma_{270}\},$$

这里 σ_i 是绕一固定直线旋转 i° 的空间旋转，如果命

$$1\to\sigma_0,\quad i\to\sigma_{90},\quad -1\to\sigma_{180},\quad -i\to\sigma_{270},$$

显然这映射是 G 射到 G' 的同构，因此 $G\simeq G'$. 又 §2.1 习题 3 中 6 元群与对称群 S_3 同构.

再假如 M 是所有实数组成的乘集，它的结合法是普通加法，M' 是所有正实数组成的乘集，它的结合法是普通乘法，那么

$$a\to\sigma(a)=10^a$$

就是 M 射到 M' 的同构. 这是因为，对于 M 中任意元 a，它在 M' 中的像是 10^a. 反过来，对于 M' 中任意元 b，它在 M 中的像源是 $\log_{10}b$，并且当 $10^{a_i}=10^{a_j}$ 时，$a^i=a^j$，所以 σ 是 M 射到 M' 的双射. 再因为 $\sigma(a_i)=10^{a_i}$，$\sigma(a_j)=10^{a_j}$，所以

$$\sigma(a_i+a_j)=10^{a_i+a_j}=10^{a_i}\cdot 10^{a_j}=\sigma(a_i)\cdot\sigma(a_j).$$

因此 $M\simeq M'$.

又由 §2.2 定理 4，我们容易验证，循环群 (a) 假如是无穷群，那么它与整数加群 $\mathbf{Z}$ 同构，这时 $a^i\to i$ 是它们的同构映射. 假如是元数为 n 的有穷群，那么它与 $\mathbf{Z}$ 关于 (n) 的同余加群 $\bar{\mathbf{Z}}=\mathbf{Z}-(n)$ 同构，这时它们的同构映射是 $a^i\to\bar{i}$. 因此任意两个无穷循环群都同构，有穷循环群只要它们的元数相等也都同构.

由 §2.1 习题 10，我们得知，群 G 的所有变换 $\sigma_a(g)=ag$，$a\in G$，组成群 G'. 假如命 a 与 σ_a 相对应，即 $a\to\sigma_a$，那么这对应显然是 G 射到 G' 的双射；又因为 $\sigma_{ab}=\sigma_a\sigma_b$，所以它又是 G 到 G' 的同构，

因此 $G\simeq G'$．于是，我们有下面的卡莱定理.

定理 1 任意群与它的变换群的子群同构.

当 G 是有穷群时，命 $G=\{a_1,a_2,\cdots,a_n\}$，那么变换 σ_a 就是排列

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aa_1 & aa_2 & \cdots & aa_n \end{pmatrix},$$

因此，G 就与对称群 S_n 的子群同构，也就是说，任意有穷群与对称群的子群同构.

1942 年汤璪真（1898—1951）发表了这样一个定理，假定 G 是群，u 是其中任意元，如果对于 G 中任意元 a,b，规定另一个结合法：$a\cdot b=au^{-1}b$，那么 G 中元对于这种结合法形成与 G 同构的群，u 是它的单位元，$a\to au$ 是它们的同构映射[14]. 读者试根据定义加以验证.

要注意的是两个乘集 M,M' 假如同构，我们最少有一个 M 射到 M' 的同构映射，但是这种映射一般不只一个，譬如，在前面的同构映射 $a\to 10^a$ 中，如果把 10 换成任意正整数 $b(\neq 1)$，显然 $a\to b^a$ 也是它们的同构映射.

假如两个乘集 M,M' 同构，$M\simeq M'$，那么 M,M' 的乘法表，除元素的记号及行、列的顺序外，在构造上完全是一样的. 因此，假如在 M 的元素间有一个用结合法表示的性质，那么在 M' 的元素间也有一个完全与它类似的性质；反过来也成立. 因为我们讨论 M,M' 是讨论 M,M' 中元素间运算的性质，所以两个同构的群是构造相同的群，它们在本质上没有区别，也就是说，同构的群只用群的性质是无法区别它们的. 于是同构的群就可以看成是相同的群，因此一个群如果能够使它与已经研究清楚了的群同构，那么这个群也就是研究清楚了的. 同构之所以重要主要在此. 于是研究一个群时常常把它分成若干个不同构的类来讨论. 譬如 4 元群可以分为循环群及克莱茵 4 元群两类，6 元群可以分为循环群及对称群 S_3 两类（习题 15，16），15 元群只是循环群（§6.4），这样，4 元群、6 元

群以及 15 元群的构造就都清楚了. 但要注意的是,同构的群与相同的群是有区别的,譬如加群 Z 与所有偶数形成的群同构,但后者是前者的子群. 又如假定 H_1, H_2 是群 G 的两个正规子群,如果 $H_1 \simeq H_2$,那么 $G/H_1, G/H_2$ 也不一定同构,譬如

$$G = \langle a, b, c \rangle,$$

其中 $a^3 = b^2 = c^3 = [a,c] = [b,c] = 1, a^b = a^{-1}$, 即 $b^{-1}ab = a^{-1}$. 显然 $(a) \simeq (c)$. 我们不难证明 $G/(a) \simeq C_6, G/(c) \simeq S_3$,因此 $G/(a)$ 不与 $G/(c)$ 同构. 这里 C_6 是 6 元循环群,读者试根据定义加以验证.

上面是介绍同构,下面来讨论自同构.

在定义中,如果 $M' = M$,那么 σ 就叫做 M 的**自同构**,因此 M 的自同构就是 M 到自己的双射. 恒等映射显然是自同构. 再假如 G 是交换群,那么把 a 变成它的逆元 a^{-1}的映射是它的自同构.

我们知道,一个集的所有变换成为一个变换群,自同构是变换,是否一个乘集的所有自同构也能够形成为群? 假如它们成为群,当然这个群是变换群的子群.

定理 2 乘集 M 的所有自同构形成为群,叫做 M 的**自同构群**.

证明 假如 σ, τ 是 M 的自同构,因为 $\sigma\tau(a) = \sigma(\tau(a))$,所以

$$\sigma\tau(a_i a_j) = \sigma(\tau(a_i a_j)) = \sigma(\tau(a_i)\tau(a_j)) = \sigma\tau(a_i)\sigma\tau(a_j),$$

因此 σ, τ 的积 $\sigma\tau$ 是 M 的自同构.

再因为 $\sigma^{-1}\sigma(a) = a, \sigma\sigma^{-1}(a) = a$,所以

$$\begin{aligned}\sigma^{-1}(a_i a_j) &= \sigma^{-1}(\sigma\sigma^{-1}(a_i)\sigma\sigma^{-1}(a_j)) \\ &= \sigma^{-1}(\sigma(\sigma^{-1}(a_i)\sigma^{-1}(a_j))) \\ &= \sigma^{-1}(a_i)\sigma^{-1}(a_j),\end{aligned}$$

于是 σ 的逆 σ^{-1}也是 M 的自同构. 因此 M 的所有自同构成群,所以定理成立.

我们容易得知,群的自同构是把生成元仍然变为生成元,因此循环群(a),假如是无穷群,因为它只有 a, a^{-1}两个生成元,所以它的自同构也只有两个,一个是把 a 仍然变为 a,即恒等同构;另一

个是把 a 变为 a^{-1}，因此这时 (a) 的自同构群是 2 元循环群. 假如 (a) 是 n 元循环群，因为它有 $\varphi(n)$ 个生成元 a^r，这里 $(r,n)=1$，$r<n$，所以它有 $\varphi(n)$ 个自同构 $\sigma_r(a)=a^r$，因此，这时 (a) 的自同构群与 $\mathbf{Z}-(n)$ 中所有 $\bar{r}$，$(r,n)=1$，对于乘法形成的群，即关于模 n 的简化剩余系对于乘法形成的群同构. 于是循环群的自同构群只是交换群，但不一定是循环群[15].

当 $n\neq 6$ 时，n 个文字上的对称群 S_n 的自同构群与 S_n 自身同构，这结果早在 1895 年已由赫尔特尔(O. Hölder，1859—1931)证明，1940 年色格尔(Iruing E. Segal)给出一个简单证明[16].

不同构的群它们的自同构群也可能同构. 譬如，无穷循环群与 3 元循环群的自同构群都是 2 元群. 因此，群自身的性质不能转移到它的自同构群上.

下面，我们来介绍群的一种重要自同构.

假定 a 是群 G 中一元，那么映射

$$\sigma: g\to g'=aga^{-1}, g\in G,$$

是 G 的自同构. 这是因为，元 g 的像源是 $a^{-1}ga$，如果

$$aga^{-1}=aha^{-1},$$

那么 $g=h$，所以 σ 是 G 射到自己上的单射，即双射，再从

$$g'=aga^{-1}, h'=aha^{-1},$$

我们就有

$$(gh)'=agha^{-1}=aga^{-1}\cdot aha^{-1}=g'h'.$$

因此，σ 是 G 的自同构.

上面由一个元 a 决定的自同构 $g\to aga^{-1}$，叫**内(自)同构**，其它的自同构，叫**外(自)同构**. 元 aga^{-1} 叫做 g 用 a 得到的变形，g 与 aga^{-1} 叫做**共轭**.

假如 $\sigma(g)=aga^{-1}$，那么 $\sigma^{-1}(g)=a^{-1}ga$. 再假如 $\tau(g)=bgb^{-1}$，那么 $\sigma\tau(g)=(ab)g(ab)^{-1}$，这就是说，内同构的逆是内同构，两个内同构的乘积又是内同构，因此群 G 的所有内同构成为一个群，叫做 G 的**内同构群**.

定理 3 一个群的内同构群是它的自同构群的正规子群.

证明 假定 σ 是群的任意自同构，τ 是群的任意内同构，

$$\sigma(g)=h,\tau(g)=aga^{-1}.$$

于是

$$\begin{aligned}\sigma\tau\sigma^{-1}(h)&=\sigma\tau(g)=\sigma(aga^{-1})=\sigma(a)h\sigma(a^{-1})\\&=\sigma(a)h(\sigma(a))^{-1},\end{aligned}$$

因此 $\sigma\tau\sigma^{-1}$ 是内同构，所以定理成立.

1895 年赫尔特尔又证明了这样一个定理，在对称群中，有外同构的只有一个 S_6[17]. 因此当 $n\neq 6$ 时，对称群 S_n 的自同构群都是内同构群.

一个群没有中心，并且除内同构外没有外同构，叫做**完全群**，譬如 $n\neq 2,6$ 时，S_n 都是完全群.

假定 σ 是群 G 的自同构，H 是 G 的子群，如果 $\sigma(H)\subseteq H$，我们就说 H 对 σ **不变**. 于是群中对它的所有内同构都不变的子群就是正规子群，所以正规子群又叫做**不变子群**. 群中对所有自同构不变的子群，叫做**特征子群**. 显然，特征子群也是正规子群. 循环群的子群都是特征子群.

共轭也是重要的概念，下面是它的基本性质.

假如 a,b 是群 G 中元，如果它们共轭，那么在 G 中至少有一个元 g，使得 $a=gbg^{-1}$，也就是说，G 有一个内同构把 b 变成 a. 如果 G 是交换，任意元就只能够与它自身共轭. 假如 a 与它的所有共轭元相等，那么 a 就在 G 的中心中. 显然，相互共轭的元其阶数是相等的.

我们很容易证明共轭这个关系是一个等价关系，因此一个群也可以根据共轭这个关系来分类. 群中与一个元共轭的所有元成为一个类. 这种类我们又叫做**共轭类**.

假定群 G 的元数为 n，我们把 G 分为共轭类，其中由 1 个元形成的共轭类的个数 c_0 就是 G 的中心 C 的元数，其它的共轭类假如共有 r 个，并且它们的元数分别是 $c_1,c_2,\cdots,c_r$，那么我们有

$$n=c_0+c_1+c_2+\cdots+c_r,$$

这式叫做G的**群等式**，或者叫做G的**群方程**.

譬如，S_3能够分为3个共轭类：(1)；(123)，(132)；(12)，(13)，(23)，即

$$S_3=\{(1)\}\cup\{(123),(132)\}\cup\{(12),(13),(23)\}.$$

所以S_3的群等式为$6=1+2+3$. 由这式得知，1只有加2才是6的因数，即$1+2=3|6$，所以S_3除自身及单位元群外，正规子群只能是3元子群.

同上面一样，假如H是群G的子群，那么aHa^{-1}也是G的子群，子群aHa^{-1}叫做H用a得到的**变形**. H与aHa^{-1}叫做**共轭**. 这时我们叫H，aHa^{-1}做**共轭子群**. 譬如，A_4的4个相互共轭的3西洛子群是$H=((123))$，

$$(12)(34)H(34)(12)=((142)),$$
$$(13)(24)H(24)(13)=((134)),$$
$$(14)(23)H(23)(14)=((243)).$$

假如H，K是G的共轭子群，那么G就有一个内同构把H变成K. 假如G是交换群，那么任意子群只能与它自身共轭，当$aHa^{-1}=H$时，$aH=Ha$，反过来也成立. 因此我们有

定理4 假设H是群G的子群，那么H是G的正规子群的必要充分条件是H与它的所有共轭子群相等.

下面，我们来考虑群G中子群H的共轭子群的个数. 我们知道，因为H用它的正规化子K中任意元得到的变形仍为H. 又因为对于K的左陪集aK中任意元ak，我们有

$$akH(ak)^{-1}=aHa^{-1},$$

并且如果$aHa^{-1}=bHb^{-1}$，那么$b\in aK$，所以G中H的共轭子群的个数等于K在G的指标$|G:K|$，因此不大于H在G的指标$|G:H|$. 假如G的元数是n，那么H的共轭子群的个数是n的因数. 同样我们容易证明，G中所有与其中元a能够交换的元成为子群，用$Z(a)$表示，即

$$Z(a)=\{x\mid x\in G, xa=ax\}.$$

因此 G 中与元 a 共轭的元的个数等于 $Z(a)$ 在 G 的指标

$$|G:Z(a)|.$$

上面的 $Z(a)$ 叫做 a 的**中心化子**，这概念我们推广如下：

假定 G 是群，H 是 G 的子集，那么 G 中所有与 H 中任意元能够交换的元显然形成为子群，叫做 H 的**中心化子**，用 $Z(H)$ 表示，即

$$Z(H)=\{x\mid x\in G, xh=hx, h\in H\}.$$

显然 H 的正规化子包含 H 的中心化子即 $N(H)\supseteq Z(H)$. 要注意的是，$Z(H)$ 不一定包含 H，但当 H 是交换群时，$Z(H)\supseteq H$. 同样 $N(H)$ 也不一定包含 H，当 H 是子群时，$N(H)\supseteq H$. 下面我们来证明一个重要等式 $xZ(H)x^{-1}=Z(xHx^{-1})$，$x\in G$. 因为

$$(xyx^{-1})(xhx^{-1})(xyx^{-1})^{-1}=xyhy^{-1}x^{-1}=xhx^{-1},$$

这里 $y\in Z(H)$，$h\in H$. 所以 $xZ(H)x^{-1}\subseteq Z(xHx^{-1})$. 再设 $z\in Z(xHx^{-1})$，那么 $zxhx^{-1}=xhx^{-1}z$，因此 $x^{-1}zxh=hx^{-1}zx$，所以 $x^{-1}zx\in Z(H)$，即 $z\in xZ(H)x^{-1}$，或 $Z(xHx^{-1})\subseteq xZ(H)x^{-1}$. 于是上面等式成立.

由上面的等式，我们容易得知 $Z(H)$ 是 $N(H)$ 的正规子群，此外我们还有

定理 5 正规子群的中心化子是正规子群，共轭子群的中心化子是共轭子群.

下面是**西洛第二定理**[*)]

定理 6 n 元群 G 的 p 西洛子群彼此共轭，假如它们的个数是 n_p，那么

$$n_p\mid n,\quad n_p\equiv 1 \pmod{p}$$

这是一个非常重要的定理，其证明比较麻烦，只好从略.

由共轭子群的定义，我们容易得知，假如 G 的 p 西洛子群只

---

*) 有的书中把这定理分写成两个定理，因此有所谓西洛三定理之称.

有 H 一个，那么 H 就是 G 的正规子群. 譬如 A_4 的 2 西洛子群只有 $1=1+2\cdot 0$ 个，因此 B_4 是 A_4 的正规子群；又 A_4 的 3 西洛子群共有 $4=1+3\cdot 1$ 个：

$$((123)),\ ((142)),\ ((134)),\ ((243)).$$

它们彼此共轭.

现在我们可以回转来证明 §2.3 中的西洛第一定理.

用反证法，假设定理不成立，即对于 p 有元数为

$$n=mp^r,\quad (m,p)=1$$

的群 G，它没有 p^r 元子群，在所有这样的群中，我们就假定 G 是其中元数最小的一个群.

假定 H 是 G 的真子群，如果 $p^r \mid |H|$，因为 H 的子群也是 G 的子群，所以 H 也没有 p^r 元子群，但 $|H|<|G|$，这与 $|G|$ 是最小的假设不合. 因此 $p^r \nmid |H|$. 这就是说 G 中没有元数能够用 p^r 整除的真子群. 再因为 $n=mp^r=|H||G:H|$，所以 $p \mid |G:H|$.

由群等式

$$n=mp^r=c_0+c_1+\cdots+c_r,$$

因为 c_0 是 G 的中心 $Z(G)$ 的元数，c_i 是 G 的某个子群的指标，所以 $p|c_i$. 于是我们有 $p|c_0$，即中心 $Z(G)$ 的元数是 p 的倍数. 设若对有穷交换群拉格朗日定理的逆也成立（§6.5），则在 $Z(G)$ 中必有阶为 p 的元 a，这样我们就得到 G 的正规子群 (a). 因为 $\overline{G}=G/(a)$ 的元数 $mp^{r-1}<n$ 并根据 n 是最小的假设，$\overline{G}$ 有 p^{r-1} 元子群 $\overline{K}$. 假定 K 是 $\overline{K}$ 中全部元所在的 (a) 的陪集的元集合，我们不难证明 K 是 G 的子群，其元数显然是 $p^{r-1}\cdot p$ 等于 p^r，这与 G 没有 p^r 元子群的假设矛盾. 注意到熟知的命题 $P(r)$ *)，定理得以证毕.

习　题　2.4

1. 假定 $G=\{e,a,b,c\}$ 的群表是

---

*) $P(r)$：令 $|G|=p^r$，$\forall\, k(0\leqslant k\leqslant r)$，$G$ 必有 p^k 阶正规子群.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

试证它除了恒等同构外，没有内同构，并且有五个外同构. 即克莱茵四元群的自同构群是对称群 S_3，因此交换群的自同构群不一定是交换群.

2. 证明对称群 S_3 没有外同构，但有六个内同构，并证明它的自同构群与它自身同构.

3. 试证四元数群(§2.3，习题8)与由矩阵

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

形成的 8 元群同构. 这里 i 是虚数单位.

4. 假如 $H\lhd G$，K 是 G 的子群，试证 $(H\cap K)\lhd K$.

5. 假设 H,K 是群 G 的子群，$G\supseteq K\supseteq H$，$H\lhd G$，如果 $K/H\lhd G/H$，试证 $K\lhd G$.

6. 假如 H 是群 G 的真子群，试证 G 有不在 H 的任意共轭子群中的元.

7. 试证 p 群的中心的元数大于 1，也就是说，p 群的中心仍然是 p 群. 因此 $p^n(n\neq 1)$ 元群不是单群.

8. 假如 p 是质数，试证 p^2 元群是交换群.

9. 试证非交换单群与它的内同构群同构.

10. 试证群的中心是特征子群. 换位子群也是特征子群.

11. 试证特征子群这个关系是满足传递律的，也就是说，假如 C 是 B 的特征子群，B 又是 A 的特征子群，那么 C 是 A 的特征子群.

12. 试证包含换位子群的子群是正规子群.

13. 假如 H 是群 G 的子群，K 是 H 的正规化子，试证 aKa^{-1} 是 aHa^{-1} 的正规化子，这里 $a\in G$.

14. 假定 H 是群 G 的子群，试证 $Z(H)\lhd N(H)$.

15. 试证 4 元群不同构的只有循环群及克莱茵 4 元群，因此 4 元群是交换群.

16. 试证 6 元群只有循环群及对称群 S_3 两类.

17. 试证 8 元非交换群只有四元数群及二面体群两类.

18. 假定 H 是群 G 的子群，$G=a_1H\cup\cdots\cup a_nH$，如果 $a_1,\cdots,a_n$ 中与 H 能够交换的只有 $a_1,\cdots,a_m$，那么 H 的正规化子 $K=a_1H\cup\cdots\cup a_mH$. 试用此求 $\{(1),(234),(243)\}$ 在 S_4 中的正规化子，并求它的共轭子群.

19. 试求 S_4 的 2 西洛子群 B_8 的正规子群及它的中心.

20. 试求对称群 S_4 的西洛子群，并证明它们共轭.

§2.5　同　　态

上节同构概念中的双射，假如换成一般的映射，我们就得到它的推广，这节就是讨论这推广概念的基本性质.

定义　假设 M,M' 是两个乘集，σ 是 M 射到 M' 的映射，并且对于 M 中任意两元 a,b，

$$\sigma(ab)=\sigma(a)\sigma(b),$$

那么 σ 叫做 M 到 M' 的**同态**. 如果 σ 是 M 射到 M' 内的映射，我们就叫 σ 是 M 到 M' **内的同态**. 如果 σ 是 M 射到 M' 上的映射，我们就叫 σ 是 M 到 M' **上的同态**，这时我们又说 M 与 M' **同态**，用记号 $M\sim M'$ 表示.

当 σ 是双射时，σ 就是同构，因此同构是同态的特例.
同态这个关系适合自反律，传递律，但不适合对称律，即从 $R\sim R'$ 不能推得 $R'\sim R$，因此同态不是等价关系.

在上面的定义中，如果 $M'\subseteq M$，也就是说，$\sigma(M)\subseteq M$，那么 σ 就叫做 M 的**自同态**. 假如 σ 是 M 的自同态，当 σ 是双射时，那么 σ 就是 M 的自同构.

譬如，我们把一个群的每个元都与单位元对应，那就得到群到单位元群上的同态，这同态又叫做**零同态**. 同样，我们把一个由排列组成的群中元，按照它是奇排列或者是偶排列分别对应于 -1 或者 $+1$，就得到对称群的子群射到由 $-1,+1$ 两个整数组成的群上的同态. 又如我们把每个整数 n 对应于由 a 生成的循环群 (a) 中元 a 的幂 a^n，那就得到加群 Z 射到 (a) 上的同态，当 (a) 是无穷群

时，这同态又是同构.

下面，我们讨论同态的性质. 因为同构是同态的特例，所以凡是同态具备的性质，对同构来说也同样成立.

定理 1 假定群 G 与乘集 G' 同态，那么 G' 成群. 这就是说，一个群的同态象也是群.

证明 假定 G' 中任意三元 a', b', c' 的象源分别是 G 中元 a, b, c，那么从 $ab \cdot c = a \cdot bc$，就得到

$$a'b' \cdot c' = a' \cdot b'c'.$$

也就是说，在 G' 中结合律成立. 又由 $ea = a$，我们就有

$$e'a' = a',$$

再由 $a^{-1}a = e$，又有

$$(a^{-1})'a' = e'.$$

也就是说，G' 有单位元 e'，并且 G' 中每个元 a' 也有逆元 $(a^{-1})'$，因此 G' 成群，所以定理成立.

从上面的证明我们还知道，群的同态把单位元 e 变为单位元 e'，元 a 的逆 a^{-1} 变为 a 的象 a' 的逆 $(a')^{-1}$，因此

$$(a^{-1})' = (a')^{-1}.$$

再群的同态把子群变为子群，正规子群变为正规子群，群的生成元仍然变为生成元，这些都是常常要引用的结果.

要注意的是，上述定理的逆不成立. 这就是说，假如 M, M' 同态，并且 M' 成群，那么 M 就不一定成群. 譬如 M 是所有自然数结合法是加法形成的乘集，M' 是由 $-1, +1$ 两个整数对于乘法形成的群，显然把偶数变为 1，奇数变为 -1 是 M 射到 M' 上的同态，但这时 M 不是群. 当同态是同构时，上定理的逆显然成立.

我们知道群 G 与 G' 同态，其对应关系是多对一的，G' 中元在 G 中完全象源的元数(即浓度)是否都一致? 首先我们来考虑单位元的完全象源.

定理 2 假定群 G 与群 G' 同态，那么 G' 的单位元 e' 在 G 的完全象源 E 是 G 的正规子群，叫做这同态的同态核.

证明 假定e_i,e_j是E中任意元,因为它们的象都是e',所以

$$(e_ie_j^{-1})'=e'\cdot(e')^{-1}=e',$$

于是$e_ie_j^{-1}\in E$,因此E成群. 再对于G中任意元a,因为

$$(ae_ia^{-1})'=a'e'_i(a^{-1})'=a'e'(a')^{-1}=a'(a')^{-1}=e',$$

所以

$$aEa^{-1}\subseteq E,$$

于是E是正规子群,所以定理成立.

于是假如σ是群G到群G'的同态,那么G的象$\sigma(G)$是G'的子群,σ的同态核$\ker(G)$是G的子群,并且是正规子群.

对于任意元的完全象源,我们有

定理3 假定群G与G'同态,E是同态核,G中元a在G'中的象是a',那么a'的完全象源是左陪集aE.

证明 因为左陪集aE中任意元的象都是$a'e'=a'$,所以aE中任意元都是a'的象源. 再假定b的象是a',我们从

$$(a^{-1}b)'=(a')^{-1}a'=e',$$

就得到

$$a^{-1}b\in E,$$

于是$b\in aE$,即b在左陪集aE中,所以a'的完全象源是aE,因此定理成立.

于是当$G\sim G'$时,G'中元在G中完全象源的元数是一致的. 又因为G中元素间的关系在G'中仍然类似地成立,所以G'虽然不能作为G的象,但也可以说是G的"缩影". 我们研究G的缩影,对G的性质必然有所说明,同态的重要也就在此.

假如群$G\sim G'$,E是同态核,如果E是单位元群,那么$G\simeq G'$,即G与G'同构. 再假如$G\simeq G'$,那么同态核E就是单位元群,因此同态成为同构的必要充分条件是它的同态核是单位元群.

假如G是单纯交换群,$\sigma(\neq 0)$是它的自同态,由定理1,我们容易得知$\sigma(G)$是G中异于单位元群的子群,因为G的子群只有单位元群及G自身,所以$\sigma(G)=G$,即σ是G射到自己的满射. 再这时同态核显然是单位元群,所以σ又是双射,因此σ是G的自同

构. 这就是说,单纯交换群的自同态或为零同态,或为自同构.

上面从一个同态出发就得到一个正规子群,那就是它的同态核. 现在我们从 G 的正规子群 H 出发,能否得到 G 的一个同态象? 这问题不难解答,只要我们命左陪集 aH 中任意元与商群 $\bar{G}=G/H$ 中元 $\bar{a}$ 对应,就得到 G 射到 $\bar{G}$ 上的同态,因此 G 就是我们需要的同态象. 于是我们有

定理 4 假定 H 是群 G 的正规子群,那么 G 与它关于 H 的商群 $\bar{G}=G/H$ 同态,即

$$G\sim\bar{G}$$

同态核就是 H,象这样的同态又叫做 G 射到 $\bar{G}$ 上的**自然同态**.

于是我们知道假如 G 有一个同态,它就是一个正规子群. 反过来,假如 G 有一个正规子群,它就有一个自然同态. 因此,假如 G 有一个同态,它就有一个自然同态. 说明这两个同态彼此间关系的,有下面的**同态基本定理**.

定理 5 假定群 G 与群 G' 同态,E 是同态核,那么

$$G'\simeq G/E$$

证明 因为 $G\sim G'$,假定这时的同态映射是 $a\to a'$,由上面定理 3,a' 的完全象源是 a 所在的左陪集 aE. 如果左陪集 aE 用 $\bar{a}$ 表示,命 $\bar{a}$ 与 a' 对应,即 $\bar{a}\to a'$. 因为 $a'=b'$ 时,a,b 同属 E 的一个左陪集,即 $\bar{a}=\bar{b}$,所以这对应就是 G/E 射到 G' 的双射. 再因为

$$\bar{a}\bar{b}=\overline{ab}\to(ab)'=a'b',$$

所以 $G/E'\simeq G'$,因此定理成立.

于是我们得知,任意同态象可以看成商群,任意同态可以看成是自然同态;也就是说,用正规子群能够决定所有的同态象,正规子群与自然同态是一对一的,也就是说,有多少正规子群就有多少自然同态,这是正规子群也是商群的一个重要性质.

单群是这样的群,它除自身及单位元群外,没有其它同态象.

假定二群 $G\sim G'$,同态核是 E,H 是 G 的子群,那么 H 在 G' 中的象 H' 也是 G' 的子群,这时 $H\sim H'$. 同态核就是 H 中所有在

E 中的元的集合，即同态核是 $H\cap E$，于是由上面定理5，我们有

$$H/H\cap E\simeq H'.$$

当 $H\supseteq E$ 时，$H/E\simeq H'$.

最后是关于自由群的一个重要定理.

定理6 任意群与某自由群的商群同构.

证明 假定群 G 的生成元集为 $\{a_i \mid i\in I\}$，F 是由 $X=\{x_i \mid i\in I\}$ 生成的自由群，显然映射 $x_i\to a_i$ 把 F 中的字

$$x_{\alpha_1}^{m_1}x_{\alpha_2}^{m_2}\cdots x_{\alpha_k}^{m_k}\to a_{\alpha_1}^{m_1}a_{\alpha_2}^{m_2}\cdots a_{\alpha_k}^{m_k}$$

因此这映射是 F 射到 G 上的同态，所以 $F\sim G$. 这时同态核 E 是使 G 中所有

$$a_{\beta_1}^{n_1}a_{\beta_2}^{n_2}\cdots a_{\beta_l}^{n_l}=e$$

的字

$$x_{\beta_1}^{n_1}x_{\beta_2}^{n_2}\cdots x_{\beta_l}^{n_l}$$

形成的子群，因此，$G\simeq F/E$. 即 G 与 F 的商群同构. 定理证毕.

于是自由群在某种意义下概括了所有的群，所以非常重要.

习 题 2.5

1. 试证对称群 S_4 关于克莱茵四元群 B_4 的商群 S_4/B_4 与 S_3 同构.

2. 假如群 G 与群 G' 同态，它的核是 E，试证 G 中任意两元在 G' 中有相同的象的必要充分条件是：它们同在 E 的一个陪集中.

3. 试证群 G 的 内同构群与 G 关于其中心 $Z(G)$ 的商群 $G/Z(G)$ 同构. 因此非交换群的自同构群不是循环群.

4. 单群的同态象是单群或者单位元群.

5. 试证 G/E 的任意子群是 H/E，这里 H 是 G 的子群，并且 $H\supseteq E$.

6. 假定 G 是群，如果 $G/Z(G)$ 是循环群，那么 G 是交换群.

7. 假定 N 是群 G 的正规子群，如果 N 是有穷，G/N 也是有穷，试证 G 是有穷群.

8. 一个群如果其中任意有穷个元生成的子群都是有穷群，那么它叫做局部有穷群，显然有穷群是局部有穷群，局部有穷群的子群是局部有穷群.

假如 N 是群 G 的正规子群，如果 N 及 G/N 都是局部有穷群，试证 G 也是局部有穷群.

9. 假定 M, M' 是两个乘集，σ 是 M 射到 M' 上的可逆映射，如果对于 M 中任意元 a, b，有 $\sigma(ab)=\sigma(b)\sigma(a)$ 那么这 σ 叫做 M 射到 M' 上的逆同构. 试证任意群与它自身逆同构.

10. 假定 G 是群，a 是 G 中一元，试证 $\tau_a(g)=ga, g\in G$，是 G 的一个变换，并且 G 的所有这样的变换形成一个与 G 逆同构的群.

参 考 文 献

[1] 乘航，纪念伽罗华诞生 150 周年，数学通报，7(1961)，39～40.

[2] C. Johnson, A mixed non-group, Amer. Math. Monthly, 71(1964), 785.

S. D. Chatterji, Product of all elements in a finite abelian group, Amer. Math. Monthly, 71(1964), 1142～1143.

[3] Paul Lorenzen, Ein Beitrag zur Gruppenaxiomiatik, Math. Z., 49 (1944), 313～327.

陈重穆、金民勇：关于群的定义，数学进展，4(1958)，127～131.

S. Michael, A single postulate for groups, Amer. Math. Monthly, 68 (1961), 346～347.

[4] W. Phillips, On the definition of even and odd permutations, Amer. Math. Monthly, 74(1967), 1249～1251.

[5] F. Szásg, On cyclic groups, Fund. Math., 43(1956), 238～240.

J. H. E. Cohn, A condition for a finite group to be cyclic, Proc. Amer. Math. Soc.. 32(1972), 48.

F. M. Sioron, A condition for semigroup to be an abelian group, Amer. Math. Monthly 71(1964), 1133～1134.

郭元春，关于 szárz 的一个定理，吉林大学自然科学报，1984 年第 2 期.

[6] G. A. Miller, Collected works, vol. 3. University of Illinois Press, Urbcna (1946).

[7] G. A. Miller, Groups which contain ten or eleven proper subgroups, Proc. Nat. Acad. Sci. U. S. A., 25(1939), 540～543.

[8] Humphreys, J. F., On groups satisfying the converse of Lagrange's Theorem, Proc. Cambridge Philos. Sec. 75(1974), 25～32.

[9] M. 赫尔：群论(裘光明译),52~53.

[10] A. F. 库洛什,群论(曾肯成、郝炳新译), § 9.

[11] L. E. Dickson, Linear groups, with exposition of the Galoisfield theory, 309~310.

C. Cato, The orders of the known simple groups as far as one Trillion, Math. Comp., 31, No. 138(1977), 574~577.

[12] W. Feit and J. G. Thompson, Solvability of Groups of edd order. Pacific Jour. of Math., vol. 13, No. 3(1963).

[13] O. Ore, Some remarks on comnutators, Proc. Amer. Math. Soc., 2 (1951), 307~314.

曾肯成、徐诚浩,关于两类有限单群中的换位元,数学进展,8(1965). 202~208.

[14] 汤璪真,群之新基本特征,武汉大学理科季刊,第 8 卷,第 1 期(1942).

[15] John Stout, Automorphisms of cyclic group, Amer. Math. Monthly 71 (1964), 568.

[16] Irving E. Segal, The automorphisms of symmetric group, Bull, Amer. Math. Soc., 46(1940), 565.

[17] G. W. Miller, On a theorem of Hölder, Amer. Math. Monthly, 65 (1958), 252~254.

P. J. Lorimer, The outer automorphisms of S_6, Amer. Math. Monthly, 73(1966), 642~643.

第3章

环　与　体

这章介绍环与体的基本概念，并且详细地叙述环的一些基本性质，最后讨论环中元素的因子分解等问题. 这章是以环为主，关于域及一般环，以后还要详细讨论.

§3.1　环的概念

在上章，我们已经认识了群. 群是只有一种结合法的代数系，也就是说，在群中任意两个元只有一种结合法. 现在来讨论有两种结合法的代数系. 在有两种结合法的代数系中，环与体是最基本的.

定义1　一个非空集合 R，假如它有两种结合法，一种叫做加法(用记号＋表示)，一种叫做乘法(用记号 · 表示)，并且还满足下面三个条件时，就叫做环：

1°　对于加法成为交换群，叫做 R 的加群；

2°　对于乘法成为半群，叫做 R 的半群；

3°　对于加法及乘法适合分配律，即对于 R 中任意三元 a,b,c，有

$$a(b+c)=ab+ac,\ (b+c)a=ba+ca.$$

于是，环是这样的代数系，其中任意两元对于加、减(加法的逆运算)、乘三个结合法能够任意施行. 一个环如果又满足乘法的交换律，即

$$ab=ba,$$

就叫做交换环．同群的情况一样，元数是有穷的环，叫做有穷环．否则叫无穷环．

譬如，仅一个数0，结合法是普通加法，乘法，形成为环．整数集Z，结合法是普通加法与乘法，成为环，叫做整数环．我们知道

$$\overline{Z}_n = Z-(n)=\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$$

是加群，它的加法是$\overline{a}+\overline{b}=\overline{a+b}$．现在再来规定它的乘法为

$$\overline{a}\ \overline{b}=\overline{ab},$$

也就是说，当$ab\equiv c(n)$时，$\overline{a}\cdot\overline{b}=\overline{c}$．这规定是唯一的，因为假如$a\equiv a'(n)$，$b\equiv b'(n)$，那么$ab\equiv a'b'(n)$．我们容易证明$\overline{Z}_n$对于乘法成为半群，并且还适合分配律，因此它成为$n$元交换环，$\overline{0}$是它的零元，$\overline{1}$是它的单位元．又用整数组成的所有$n$阶矩阵($n$是固定的)形成为环，它不是交换环．一般，假如$R$是环，所有用$R$中元组成的$n$阶矩阵形成为非交换环，叫做$R$上的$n$级全矩阵环，用记号$R_n$来表示．全矩阵环是一类非常重要的环．

假定R是环，$G=\{u_1,\cdots,u_n\}$是群，结合法是乘法，我们容易证明，所有形如

$$\sum_{i=1}^{n}a_iu_i=a_1u_1+\cdots+a_nu_n,\quad a_i\in R$$

的元，根据规定

$$\sum_{i=1}^{n}a_iu_i=\sum_{i=1}^{n}b_iu_i,\quad 当\ a_i=b_i, i=1,\cdots,n.$$

$$\sum_{i=1}^{n}a_iu_i+\sum_{i=1}^{n}b_iu_i=\sum_{i=1}^{n}(a_i+b_i)u_i,$$

$$\left(\sum_{i=1}^{n}a_iu_i\right)\left(\sum_{j=1}^{n}b_ju_j\right)=\sum_{i,j=1}^{n}a_ib_ju_iu_j$$

(上式右边显然呈$\sum c_iu_i$，$c_i\in R$的形状)，形成为环，叫做G关于R的群环，用$R[G]$表示[1]．

任意加群其中任意两元的乘积如果规定为0(加群的单位元)，即乘法表全为0时，显然它成为环，象这样任意两元的乘积都

为 0 的环，叫做**零环**. 只由一个零元组成的零环，有时就简称它为零.

环 R 的子集 S，假如对于 R 的两种结合法又形成为环，那么 S 就叫做 R 的**子环**，R 叫做 S 的**扩张环**. 环的一个子集成为子环，只要它对加法成群，对乘法是闭合的就行了，因为其他条件显然都适合. 环可以看成是自身的子环，异于自身的子环叫做**真子环**. 由下面性质 1°，我们得知任意环都有只由一个零元组成的零子环. 同群的情况一样，环中与所有元能够交换的全部元形成子环，叫做环的**中心**，环 R 的中心用 $Z(R)$ 表示. 显然交换环的中心就是它自身.

有穷环显然只能有有穷个子环. 反过来也成立，即一个环如果只有有穷个子环，那么这环是有穷环[2].

上面说明了环及子环的定义，并且给出了一些例子，现在我们来讨论环的一些基本概念及基本性质.

因为环 R 对于加法成群，也就是说 R 是加群，所以我们把它的单位元写成零元 0，元 a 的逆元写成 a 的负元 $-a$. 在环中用加法表示的各种性质，也就是加群的各种性质，由第二章可以直接推得. 下面我们只讨论与乘法有关的各种性质.

零元及负元在加法中的地位由加群的性质已很清楚，它们与乘法的关系有

1° $0\cdot a=a\cdot 0=0$,

2° $(-a)\cdot b=a\cdot(-b)=-ab, (-a)(-b)=ab$,

式中 a,b 是环 R 中任意元.

这是因为由分配律

$$0\cdot a+0\cdot a=(0+0)a=0a$$

就得到

$$0\cdot a=0,$$

同样 $a\cdot 0=0$，因此 1°得证.

又因为 $\quad (-a)b+ab=(-a+a)b=0b=0,$

所以 $(-a)b$ 是 ab 的负元，也就是说，$(-a)b=-ab$. 同样，

$$a(-b)=-ab.$$

再因为

$$(-a)(-b)=-(-a)(b)=-(-ab)=ab,$$

因此2°得证.

此外，我们容易知道，

$$c(a-b)=ca-cb,(a-b)c=ac-bc,$$

这就是说，在环中对于减法的分配律也是成立的.

于是环 R 中元施行加法，减法，乘法等运算时，与普通代数中数的情况一样. 但必须注意，乘法的先后顺序不一定可以颠倒；除法（乘法的逆运算）在 R 中不一定可以施行，因此乘法的消去律也不一定成立，这就是说，从 $a\cdot b=a\cdot c$ 或者 $b\cdot a=c\cdot a$，当 $a\neq 0$ 时，我们不一定能够得到 $b=c$. 因此，从 $a\cdot b=0$，我们不一定能够得到 $a=0$ 或 $b=0$.

假如 a 是环 R 中元，如果 R 中有一元 $b\neq 0$ 存在，使 $ab=0$（$ba=0$），那么 a 就叫做 R 的左（右）零因子，有时 a 又叫做 b 的左（右）零化元. 假如 $a\neq 0$，那么 b 是 R 的右零因子. 因此 R 中非零的左、右零因子是成对出现的. 一元如果是左零因子，同时又是右零因子，就叫做零因子. 假如 a 是 R 的零因子，那么 R 中有非零元 b,c，使 $ab=0,ca=0$，但 b,c 不一定相等. 环 R 中元 a 如果不是 R 的左、右零因子，就叫做正则元，非零环的零元是当然的零因子. 一般，环中除零元外，可能还有其他零因子.

譬如，在整数环 Z 上的2阶全矩阵环 Z_2 中，非零元

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix},\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$$

都是零因子，这是因为

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}=0,\begin{pmatrix} 0 & 0 \\ b & -a \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}=0,\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}\begin{pmatrix} d & 0 \\ -c & 0 \end{pmatrix}=0.$$

定义 2 假定环 R 中除零元外既没有左零因子，也没有右零因子，那么 R 就叫做无零因子环；交换无零因子环又叫做整环.

譬如，整数环 Z 是整环. 在无零因子环中除零元外都是正则元. 显然，环成为无零因子环的必要充分条件是对于其中任意两元 a,b，如果 $ab=0$，那就有 $a=0$ 或 $b=0$. 再假如 R 是无零因子环，由 $ab=ac$ 或 $ba=ca$，当 $a\neq 0$ 时，就得到 $b=c$，这是因为 $a(b-c)=0$ 或 $(b-c)a=0$，而 $a\neq 0$，所以 $b-c=0$，即 $b=c$. 因此，在 R 中乘法的消去律成立. 反过来，假如在环 R 中乘法的消去律成立，如果其中两元 a,b 的积 $ab=0$ 而 $a\neq 0$，我们由 $ab=a0$ 就得到 $b=0$，因此 R 是无零因子环. 于是我们又得知，环成为无零因子环的必要充分条件是它满足乘法的消去律.

要注意的是无零因子环不只是没有零因子的环而且是没有左零因子也没有右零因子的环.

环中元 a，如果 $a^n=0$，这里 n 是正整数，那么 a 叫做幂零元. 零元是幂零元，非零的幂零元是零因子. 显然，在无零因子环中零元是唯一的幂零元，它没有非零的幂零元. 但反过来不一定成立，即在不含非零的幂零元的环中可能有零因子. 譬如，在 $Z-(6)$ 中，$\bar{2},\bar{3},\bar{4}$ 都不是幂零元，但却都是零因子.

一个环，其中任意元都是幂零元时，叫做幂零元环. 零环是幂零元环.

定理 1　交换环 R 中所有幂零元形成一个幂零元环.

证明　假定 a,b 是 R 中任意两个幂零元，$a^m=0,b^n=0$，因为

$$(a-b)^{m+n}=a^{m+n}-C_1^{m+n}a^{m+n-1}b+\cdots+C_n^{m+n}a^m(-b)^n$$
$$+C_{n+1}^{m+n}a^{m-1}(-b)^{n+1}+\cdots+(-b)^{m+n}=0,$$

$$(ab)^m=a^mb^m=0,$$

即 a,b 的差 $a-b$ 及积 ab 又都是幂零元，所以 R 中所有幂零元形成为环，子是定理成立.

下面，我们来讨论环中乘法的单位元及逆元.

我们知道，环对乘法可能只成为半群，所以在环的定义中，并不要求对乘法要有单位元，但在许多环中往往有这种元存在.

定义 3　假如环 R 中有元 $e_L(e_R)$，它对子 R 中任意元 a 有 e_La

$=a(ae_R=a)$，那么 $e_L(e_R)$就叫做 R 的左(右)单位元. 假如 R 中有元 e，它既是左单位元同时又是右单位元，即对于 R 中任意元 a 有 $ea=ae=a$，那么 e 就叫做 R 的单位元，这时 R 叫做有单位元环.

譬如，整数环 Z 是有单位元的环，它的单位元就是 1. 所有的偶数也成为环，叫做偶数环，但它没有单位元. 当 R 有单位元 e 时，n 阶全方阵环 R_n 也有单位元，这单位元就是单位矩阵.

$$\begin{pmatrix} e & & \\ & \ddots & \\ & & e \end{pmatrix}.$$

要注意的是，假如环有单位元，并且它的子环也有单位元，这两个单位元不一定一致. 譬如，所有形如 $\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix}$，$a$ 是整数的矩阵成为 Z_2 的子环，显然 $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ 是它的单位元，而不是 Z_2 的单位元. 但环的零元与子环的零元是一致的. 在异于零的环中，单位元不是零元.

假如环 R 有左单位元 e_L，同时又有右单位元 e_R，那么，

$$e_Le_R=e_L=e_R,$$

也就是说，e_L 或 e_R 是 R 的单位元. 因此在有单位元的环中，左单位元就是右单位元，也就是单位元，所以单位元是唯一的. 在没有单位元的环中，左单位元，右单位元不能同时存在. 假如环 R 只有一个左单位元 e_L，那么 e_L 就是 R 的单位元，这是因为对于 R 中任意元 a，显然 e_L+ae_L-a 又是 R 的左单位元，所以 $e_L+ae_L-a=e_L$，因此 $ae_L=a$，这就是说，e_L 又是 R 的右单位元，所以它是 R 的单位元.

一个环可能有不只一个左单位元而没有右单位元，同样也可能有不只一个右单位元而没有左单位元. 譬如，所有形如 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 的矩阵组成的环，它没有右单位元，但有无穷多个左单位

元

$$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix},$$

这里 a,b,c 都是整数. 同样,所有形如$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$的矩阵组成的环没有左单位元,但有无穷多个右单位元

$$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}.$$

单位元显然不是零因子,但左(右)单位元就不一定,譬如,上面的左单位元$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$就是右零因子,这是因为

$$\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

环中元 a,如果 $a^2=a$,那么 a 就叫做幂等元. 显然,左(右)单位元是幂等元. 零元当然满足上面幂等元的条件,但我们不把它看成幂等元,因此,我们所说的幂等元是异于零的元. 幂等元可能是零因子. 因此,幂等元不一定是单位元. 假如幂等元 e 不是左零因子,那么他就是左单位元,这是因为,从 $e^2=e$,我们有 $e^2a=ea$,即 $e(ea-a)=0$,所以 $ea=a$,同样假如 e 不是右零因子,那么 e 就是右单位元. 因此如果 e 是正则元,那么它就是单位元. 于是在无零因子环中,左(右)单位元都是单位元,假如它有幂等元,因为幂等元是单位元,那么单位元就是唯一的幂等元了.

一环,其中任意非零的元都是幂等元时,就叫做布尔(G. Boole,1815~1864)环[3]. 譬如,Z-(2)就是布尔环.

纵然环 R 有单位元 e,但当 $a\in R$ 时,对乘法,a 也未必就有左(右)逆元.

定义 4 假设环 R 有单位元 e,对于 R 中元 a,如果有元 a_L^{-1} (a_R^{-1})存在,使 $a_L^{-1}a=e$ ($aa_R^{-1}=e$),那么 a_L^{-1} (a_R^{-1})就叫做 a 的左(右)逆元. 如果有元 a^{-1},它既是 a 的左逆元,同时又是 a 的右逆

元，即 $a^{-1}a=aa^{-1}=e$，那么 a^{-1} 就叫做 a 的逆元.

在有单位元的环中，每一元未必都有逆元. 有逆元的元，叫做**可逆元**. 譬如，零元 0，它就没有逆元. 单位元 e 的逆元就是它自身. 如果 a 有逆元 a^{-1}，那么 a^{-1} 的逆元就是 a；再如果 a 有逆元 a^{-1}，b 有逆元 b^{-1}，那么 ab 的逆元就是 $b^{-1}a^{-1}$. 即

$$(a^{-1})^{-1}=a,(ab)^{-1}=b^{-1}a^{-1}.$$

零元固然没有逆元，就是零因子同样也没有逆元. 这是因为，假如 a 是零因子，$ab=0,b\neq0$，如果 a 有逆元 a^{-1}，那么 $a^{-1}ab=0$，于是 $eb=b=0$，这与假设不合，所以 a 没有逆元. 因此，如果 a 有逆元，那么它是正则元，就不是零因子.

假如 a 是幂零元，$a^n=0$，当然 a 没有逆元，如果环 R 有单位元 1，那么 $1-a$ 是可逆元，这是因为

$$(1-a)(1+a+\cdots+a^{n-1})=(1+a+\cdots+a^{n-1})(1-a)=1$$

假如 a 是幂等元，1 是 R 的单位元，那么 $1-a$ 也是幂等元，这是因为

$$(1-a)(1-a)=1-a-a+a^2=1-a.$$

如果 a 又是可逆元，那么 $a=1$，因为如果 $aa'=1$，我们就有

$$a=a\cdot aa'=a^2a'=aa'=1,$$

即幂等元如果又是可逆元，那么它就是 R 的单位元.

同单位元的性质类似，如果 a 有左逆元 a_L^{-1}，同时又有右逆元 a_R^{-1}，那么它就有逆元 $a^{-1}=a_L^{-1}=a_R^{-1}$，这是因为

$$a_L^{-1}=a_L^{-1}e=a_L^{-1}aa_R^{-1}=ea_R^{-1}=a_R^{-1}.$$

因此，一个元 a 如果有逆元，它的左逆元就是右逆元也就是逆元，所以它的逆元是唯一的. 一元可能有几个左逆元而没有右逆元，同样也可能有几个右逆元而没有左逆元. 一元如果只有一个左逆元，那么，它就有右逆元，因此它就有逆元. 这是因为，假如有 a_L^{-1}，由 $(a_L^{-1}+aa_L^{-1}-e)a=e$，我们就有 $a_L^{-1}+aa_L^{-1}-e=a_L^{-1}$，即 $aa_L^{-1}=e$，所以 a_L^{-1} 也是右逆，因此，a^{-1} 就是逆元. 假如一元有一个以上的左(右)逆元，那么它就有无穷多个左(右)逆元[1]，但在无零因子环

中，如果 a_L^{-1}，a_R^{-1} 有一存在，那么他一也存在．譬如有 a_L^{-1}，因为 $a_L^{-1}a=e(aa_L^{-1}-e)=0$，所以 $aa_L^{-1}=e$，因此 a^{-1} 也存在．

定理 2 在有单位元的环 R 中，所有可逆元对乘法形成为群 G．

证明 因为两个可逆元的乘积仍然是可逆元，所以 G 适合群定义的条件 1°．由环的定义，显然 G 适合群定义的条件 2°．R 的单位元也就是 G 中乘法的单位元，又 a^{-1} 就是 a 的逆，因此 G 成群，所以定理得证．

譬如，在整数环 Z 中，可逆元只有 $1,-1$ 两数，它们对乘法显然成群．又如在全矩阵环 Q_n 中，任意 n 阶满秩矩阵都有逆矩阵，因此 Q_n 中所有 n 阶满秩矩阵对乘法成为群．它就是线性群．再如在环 $\overline{Z}_6=Z-(6)$ 中，$\overline{2},\overline{3},\overline{4}$ 都是零因子，因此它们都不是可逆元；$\overline{1}$ 的逆元是 $\overline{1}$，$\overline{5}$ 的逆元是 $\overline{5}$，因此，在 $\overline{Z}_6$ 中所有可逆元成为元数为 2 的循环群．

上面得到的单位元以及逆元的性质，只是由环对乘法成半群这性质推得的，因此一个半群也有这些性质．

习 题 3.1

1．假定 R 是实数集，加法＋是普通的加法，但乘法×是

$$a\times b=|a|b,$$

这时 R 是否成环？

2．假设 R 是所有有理数对 (a_1,a_2) 的集合，它们的结合法是

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),$$

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,a_2b_2),$$

那么 R 是否成环？它有无零因子？是否有单位元？哪些元有逆元？

3．假定 R 是有单位元 1 的环，

$$a\oplus b=a+b-1, a\odot b=a+b-ab,$$

试证 R 对结合法 $\oplus$，$\odot$ 也成为一个有单位元的交换环．

4．试证在有单位元的环中加法的交换律可由其它条件推出，也就是说它们不是独立的．

5. 假设 $a=\begin{pmatrix}0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots\end{pmatrix}$, $b=\begin{pmatrix}0 & & & \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & \ddots\end{pmatrix}$,

$$c=\begin{pmatrix}a_1 & a_2 & & \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & \ddots\end{pmatrix}, \quad e=\begin{pmatrix}1 & & \\ & 1 & \\ & & \ddots\end{pmatrix}$$

是四个无穷阶矩阵，试证

$$ab=e, ba\neq e, ac=e,$$

即在由整数组成的无穷阶矩阵形成的环中，元 a 有无穷多个右逆，但没有左逆. 再证明 b 有无穷多个左逆，但没有右逆. 并且 a 是左零因子而 b 是右零因子.

6. 假如 R 不是零环，a 是 R 的左(右)零因子，那么 a 或是没有右(左)逆元，或是最少有两个右(左)逆元.

7. 试证在有穷环中正则元都是可逆元，也就是说，有穷环如果有正则元，它就有单位元.

8. 假如 e 是环 R 的左单位元，如果 R 没有左零因子，那么 e 是 R 的单位元.

9. 假定环 R 有单位元，E 是全矩阵环 R_n 的单位元，试证 R_n 的中心

$$Z(R_n)=Z(R)E.$$

10. 假定环 R 没有非零的幂零元，试证 R 的幂等元都在它的中心里面.

11. 试证布尔环是交换环.

12. 求元数最小的非交换环[5].

§3.2 体的概念

在近世代数中，除了群、环外，体是一个最基本的概念.

定义 一个环 F，假如含有非零的元，即至少包含两个元，并且所有非零的元对乘法成为群，就叫做**体**，有时又叫做**可除环**. 这对乘法形成的群，又叫做 F 的**乘群**. 当 F 是交换时，F 就叫**交换体**，或者叫做**域**.

于是我们得知，体有加法、乘法两种运算，并且所有元对加法成加群(交换群)，所有非零元对乘法成群，但不一定是交换群. 联系加法与乘法的就是分配律. 因此体中任意两元能够任意施行加、减、乘、除，只是零元不能除任意元.

一个体 F 至少包含两个元，一个是加群的零元，一个是乘群的单位元，每个非零的元都有逆元，所以它是正则元而不是零因子. 于是，F 是无零因子环，因此，当 F 是域时，它又是整环.

现在我们给出一些例子.

譬如，有理数集 Q 成为域，叫做有理数域. 所有有理复数 $a+bi$(a,b 是有理数)集也成为域叫做高斯(C. F. Gauss，1777～1855)数域. 同样，实数集，复数集都成为域分别叫做实数域，复数域.

只包含有穷个元的体，叫做有穷体. 将来(§5.8)我们还可以知道，任意有穷体都是域. 下面我们举一个有穷域的例子.

假如 p 是质数，那么 $\bar{Z}=Z-(p)$ 就是元数为 p 的有穷域. 这是因为当 $(a,p)=1$ 时，同余方程 $ax\equiv1(p)$ 有解，因此 $\bar{Z}$ 中任意非零元都有逆元，所以 $\bar{Z}$ 成体. 但数服从乘法的交换律，于是 $\bar{Z}$ 是域. 要注意的是，当 n 不是质数时，$Z-(n)$ 中有零因子因此它不成体，于是 $Z-(n)$ 成为域的必要充分条件是 n 为质数.

历史上第一个是体不是域的例子是 1843 年由汉弥尔顿提出的. 他先建立一种比复数更广泛的数：$ae+bi+cj+dk$，这里 a,b,c,d 是实数；汉弥尔顿叫它做四元数. 为了简便，象 $ae+0i+0j+0k$ 我们写成 ae，$0e+0i+1j+0k$ 写成 j 等等. 我们希望所有这样的实四元数能够成为体. 首先我们规定 e,i,j,k 的乘法表

	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

再规定它们的相等，相加及相乘等关系：

(1) $ae+bi+cj+dk=a'e+b'i+c'j+d'k$，当：

$$a'=a, b=b', c=c', d=d',$$

(2) $(ae+bi+cj+dk)+(a'e+b'i+c'j+d'k)$

$$=(a+a')e+(b+b')i+(c+c')j+(d+d')k,$$

(3) $(ae+bi+cj+dk)(a'e+b'i+c'j+d'k)$是将它依分配律展开，然后把各项的实系数合并，譬如$(ai)(bj)=ab(ij)$，再用上面规定的乘法结果代入得到的四元数.

对这样规定的结合法，我们很容易证明上面的所有实四元数形成为环，它是非交换环，e是它的单位元，再因为

$$(ae-bi-cj-dk)(ae+bi+cj+dk)=(a^2+b^2+c^2+d^2)e,$$

所以，对于每个非零元$ae+bi+cj+dk$都有逆元

$$(a^2+b^2+c^2+d^2)^{-1}(ae-bi-cj-dk),$$

因此它们形成为体，叫做**实四元数体**，它是非交换体.

汉弥尔顿得到上面的乘法表花费了十年时间，四元数的出现对以后其它超复数体系的发展是有重大影响的.

下面是体的一些重要性质.

体是无零因子环，它的逆一般不成立，但对有穷环是成立的，即

定理1 元数大于1的有穷无零因子环是体.

证明 由§3.1无零因子环中非零元满足乘法的消去律. 再由§2.1定理3，它对除法是闭合的，因此，环中所有非零元对乘法成群. 所以这环成体. 定理得证.

于是，有穷环如果不是体，它就含有零因子. 再在有穷环中不是零因子的元都是可逆元，即任意无逆元的元都是零因子[6]. 假如有穷环没有非零的幂零元，并且只有一个幂等元，那么这环就是体[7].

1964年根山(N. Ganesan)给出了有穷环的元数与其所含零

因子的个数之间一些关系[9]，但有穷环详细的构造现在我们还不完全清楚.

我们知道，环成为体，只要它的所有非零元对乘法能够成群，因此由§2.1定理2，如果对于环 R 中任意两元 $a(\neq 0),b$，方程 $ax=b,ya=b$ 在 R 中有解，那么 R 就是体. 下面，我们来证明上面两个方程只要一个有解就行了.

定理2 环 R 成体的必要充分条件是：对于 R 中任意两元 $a\neq 0,b$，方程 $ax=b$(或 $xa=b$)在 R 中有解.

证明 因为条件的必要性显然成立，我们只证明充分性.

假定 a,b 是 R 中任意非零的两元，从 $ax=b,by=x$，我们有

$$aby=ax=b,$$

于是 $ab\neq 0$，这就是说，R 中任意非零的两元的积仍然是非零的元，因此 R 是无零因子环. 又由 $ae=a$，我们有

$$a(e^2-e)=0,$$

于是 $e^2=e$，这就是说，e 是无零因子环 R 的幂等元，所以 e 是 R 的单位元. 再从 $aa'=e$，得知 a' 是 a 的右逆元，但 R 是无零因子环，因此 a' 也是 a 的逆元. 于是 R 中所有非零的元对乘法成群，因此 R 是体，充分条件成立，所以定理得证.

假定 K 是体，K 的子集对 K 的两种结合法成为体，叫做 K 的子体，于体是域时，又叫做子域. K 中与所有元能够交换的全部元形成的子域，叫做 K 的**中心**. 同§2.4中一样，K 中所有与子体 F 中任意元能够交换的元形成 K 的子体，叫做 F 的**中心化子**，用 $Z(F)$ 表示，即

$$Z(F)=\{x\mid x\in K,xy=yx,y\in F\}.$$

假定 F 是体 K 的子域，如果 K 中除 $F(\neq K)$ 外没有包含 F 的真子域，那么 F 叫做 K 的**极大子域**，当 K 是域时，我们把 K 自身也看成 K 的极大子域. 因为 K 的中心是子域，由冲恩(M. Zorn,

1906)引理*)，我们容易得知，任意 K 有极大子域. 假如 F 是 K 的极大子域，那么 F 包含 K 的中心 Z，这是因为，如果 F 不包含 Z，那么由 F，Z 生成的域(§4.1)显然包含 F，这与 F 是极大的假设矛盾.

极大子域是一个重要概念，在讨论非交换体时特别需要，下面是一个必要充分条件.

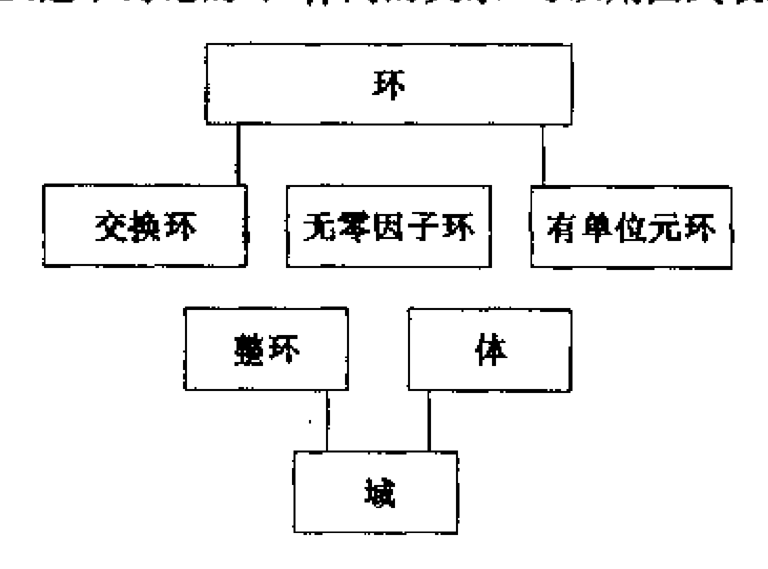
定理3 假定 F 是体 K 的子域，那么 F 是极大子域的必要充分条件是 F 的中心化子是 F 自身，即 $F=Z(F)$.

证明 假定 $F=Z(F)$，如果 K 的子域 $L\supset F$，那么 $L\subset Z(F)=F$，因此 $L=F$，即 F 是极大子域.

反过来，假如 F 是 K 的极大子域，$a\in Z(F)$，那么由 F，a 生成的子体包含 F，因此 $a\in F$，于是 $Z(F)\subseteq F$，所以 $Z(F)=F$.

定理证毕.

上节及这节讨论的环、体间的关系，可以用图式表示如下：



*) 假定 M 是由某集合的若干子集形成的系，L 是 M 的子集，如果 L 中任意两元 L_1，L_2 不是 $L_1\subseteq L_2$，便是 $L_2\subseteq L_1$ 那么 L 叫做 M 的链. 冲恩引理：假定 M 的每个链中元的并集仍是 M 中元，那么 M 中有不包含于其他元的元，即极大元.

习　题　3.2

1. 试作由两个元组成的体.
2. 假如 n 不是质数,那么 $Z-(n)$ 就不成为体,为什么?
3. 试证所有系数是复数的四元数只能成为环而不能成为体.
4. 试证体中任意有穷子环是子体.
5. 假如 $K=Z-(2)$,试证 $GL(2,K)=SL(2,K)$.
6. 假定 a,b,c 是四元数环中任意元,试证 $(ab-ba)^2c=c(ab-ba)^2$.

§3.3　同态、同构

我们已经知道群的同态、同构,这节我们把它推广到环、体上面来.

定义　假定 R,R' 是两个环,σ 是 R 射到 R' 的映射,如果对于 R 中任意元 a,b,我们有

$$\sigma(a+b)=\sigma(a)+\sigma(b),\sigma(ab)=\sigma(a)\sigma(b),$$

那么映射 σ 就叫做 R 到 R' 的**同态**.如果 σ 是 R 到 R' 内的映射,我们就叫 σ 是 R 到 R' **内的同态**,如果 σ 是 R 射到 R' 上的映射,我们就叫 σ 是 R 到 R' **上的同态**,这时我们又说 R 与 R' **同态**,用记号 $R\sim R'$ 表示.如果 σ 更是单射,即是可逆的,它就叫做**同构**,这时 R 叫做与 R' **同构**,用 $R\simeq R'$ 表示.

譬如,任意环 R 都与由零元形成的零环同态,因为我们把 R 中所有元都与零元对应就是零同态.又如

$$Z_8=\{\bar{0},\bar{1},\cdots,\bar{7}\}\sim Z_4=\{\bar{0}',\bar{1}',\bar{2}',\bar{3}'\}$$

这是因为由计算可以验证,下面的对应是它们的同态,

$$\bar{0}\to\bar{0}',\bar{1}\to\bar{1}',\bar{2}\to\bar{2}',\bar{3}\to\bar{3}',$$
$$\bar{4}\to\bar{0}',\bar{5}\to\bar{1}',\bar{6}\to\bar{2}',\bar{7}\to\bar{3}'.$$

再假如 K 是高斯数域,K' 是由所有形如 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ 的矩阵组成的体,其中 a,b 是有理数,命

$$a+bi\to\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

显然，这对应是 K 射到 K' 的双射；再因为

$$(a+bi)+(c+di)=(a+c)+(b+d)i,$$

$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i,$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\cdot\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix},$$

所以这映射又是同构，因此 $K\simeq K'$.

两个有单位元的环，元数都为 n，如果 n 没有平方数因子，那么这两个环同构[9].

同讨论群的情形一样，同构关系是等价关系，同态关系不是等价关系，同态满足自反律，传递律，但不满足对称律.

两个同构的环除了记号外，构造完全一样，也就是说，它保持原来环中用加法、乘法两种结合法表示的一切代数性质，所以我们有时也把同构的环看成是相同的环. 但同态就不是这样，它不一定保持原有的性质. 譬如 $R\sim R'$ 时，假如 R 有单位元，那么 R' 也有单位元，但反过来就不一定成立. 再假如 R 是交换环，那么 R' 也是交换环，但反过来又不一定成立. 又假如 R 是无零因子环，R' 中可能有零因子；反过来，假如 R' 是无零因子环，R 中也可能有零因子，因此 R 是整环时，R' 不一定是整环，反过来，R' 是整环时，R 也不一定是整环，譬如 $Z\sim\bar{Z}_6$，但 Z 是整环，而 $\bar{Z}_6$ 有零因子. 又如所有形如 $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$ 的矩阵，这里 a,b,c 都是整数，组成环 R，根据 $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\to a$，我们容易验证它与整数环 Z 同态，即 $R\sim Z$，这时 R 是非交换环，并且有非零的零因子.

因为环的同态也是把环看成加群时的同态，所以它把零元变

为零元，一元的负元变为这元的象的负元，因此两元的差变为它们的象的差. 又由定义，我们容易得知环的同态把幂零元变为幂零元，幂等元变为幂等元. 假如环有单位元，那么单位元也变为单位元，因此，一元的逆又变为这元的象的逆.

同群一样，环也有自同态、自同构. 我们容易得知，整数环及有理数域的自同构都只是恒等同构. 即任意元与自己对应的同构. $a+bi\to a-bi$ 是复数域的自同构. 由可逆元 a 决定的自同构 $x\to axa^{-1}$，叫做内(自)同构，不是内(自)同构的自同构，叫做外(自)同构. 实四元数体的自同构是内同构[10]. 对于任意内同构不变的子环，叫做不变子环. 我们知道，在一个非交换体中，它自身及包含在它中心的子体都是不变子体. 反过来也成立，也就是说，在一个非交换体中，不变子体只有它自身及包含在它中心的子体. 这个逆是1947 年卡登(H. Cartan，1904～)就关于中心是有穷次体(§5.3)的特殊情形首先证明，1949 年布劳尔(R. Brauwer，1901～)、华罗庚(1910～1986)同时把它推广到一般体，因此这个逆就叫做卡登—布劳尔—华罗庚定理[11].

我们将来(§3.6)还可以证明，体的非零同态都是同构，也就是说，在上面定义中，R，R' 如果都是体，我们可以证明 σ 是可逆的.

群的所有自同构成为自同构群，对于环也希望能有与这类似的自同态环. 我们知道，环 R 的自同态 σ,τ 的乘积 $\sigma\tau(a)=\sigma(\tau(a))$ 是 R 的自同态，但和 $(\sigma+\tau)(a)=\sigma(a)+\tau(a)$ 不是 R 的自同态，因为

$$(\sigma+\tau)(ab)\neq(\sigma+\tau)a\cdot(\sigma+\tau)b,$$

所以 R 的所有自同态不可能形成为环. 这样我们只有把 R 看成加群来讨论.

假定 G 是加群，σ,τ 是它的自同态，因为 $\sigma\tau(a)=\sigma(\tau(a))$，由§2.4 我们得知，$\sigma,\tau$ 的乘积 $\sigma\tau$ 是 G 的自同态. 现在我们更规定

$$(\sigma+\tau)(a)=\sigma(a)+\tau(a),$$

显然 σ,τ 的和 $\sigma+\tau$ 也是 G 的自同态，并且容易证明，加法的交换律，结合律及分配律都成立. 再我们又有

$$0(a)=0,-\sigma(a)=\sigma(-a),$$

因此 G 的所有自同态成为有单位元的环，叫做 G 的自同态环.

显然，单位元群的自同态环是由零元组成的零环，即零. 无穷循环群的自同态环与整数环 Z 同构. n 元循环群的自同态环与 $Z_n=Z-(n)$ 同构. 因此元数是质数 p 的循环群的自同态环就是域 Z_p. 一般我们有：

定理 1 元数大于 1 的单纯加群的自同态环是体.

这是因为由 §2.5 我们得知，单纯加群的异于零的自同态是自同构.

假如把环看成加群，那么它也有自同态环，于是，任意环都有自同态环. 但要注意的是，这里所说的自同态是把环看成加群时的自同态，并不是环的自同态. 环的自同态很多时候指的是把环看成加群时的自同态，并不是看成环时的自同态.

假定 R 是环，a 是其中一元，显然映射 $\sigma_a(r)=ar$ 是把 R 看成加群时的自同态，因为 $\sigma_{a+b}=\sigma_a+\sigma_b$，$\sigma_{ab}=\sigma_a\cdot\sigma_b$，所以，所有这样的自同态 σ_a 形成环 R'. 根据定义，我们容易证明，$a\to\sigma_a$ 是 R 到 R' 上的同态. 当 R 有单位元或无零因子环时，这同态又是同构，这是因为由 $\sigma_a=\sigma_b$，我们就有 $ar=br$，如果 R 是无零因子环，就得到 $a=b$，如果 R 有单位元 e，就得到 $ae=be$，因此也有 $a=b$，于是我们有

定理 2 假定 R 是有单位元的环(或无零因子环)，a 是其中一元，$\sigma_a(r)=ar$，那么 R 与所有自同态 σ_a 形成的环同构.

将来(§3.4 习题 3)我们还知道，一个没有单位元的环可以看成为一个有单位元环的子环，或者说，一个没有单位元的环可以嵌入一个有单位元的环. 这样，我们就得到下面与 §2.4 中卡莱定理类似的定理.

定理 3 任意环与某环的自同态环的子环同构.

于是任意环可以嵌入某环的自同态环.

下面是我们常常引用的挖补定理.

定理 4 假设 R' 与 S 是两个没有公共元[*]的环，并且 S 含有一个与 R' 同构的子环 R，那么，我们有一个包含 R' 并且与 S 同构的环 S'，这就是说，这时我们简直可以把 R' 看成是 S 的子环.

这定理的含义我们可以用下面的图形(图 3.1)来表示.

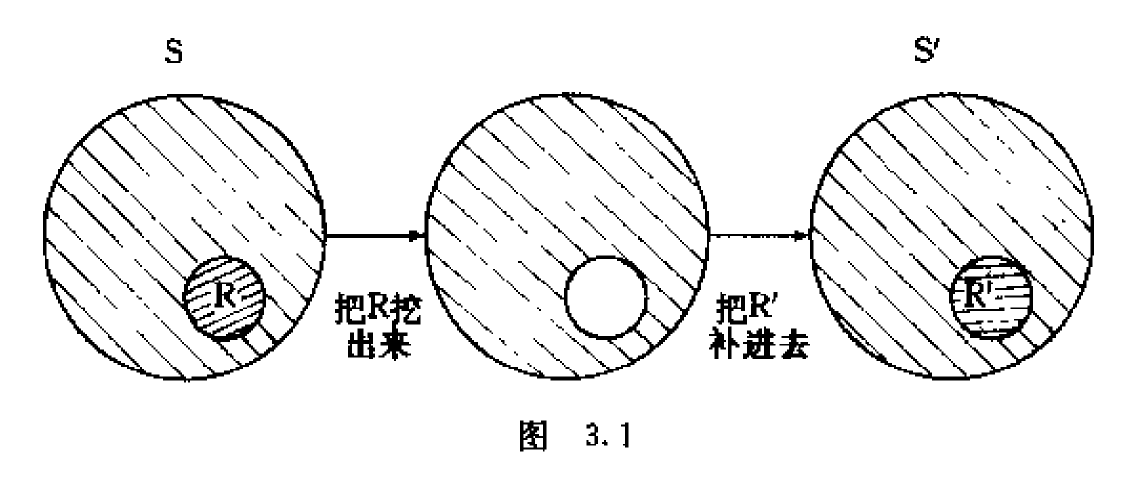


图 3.1

证明 我们命

$$S'=R'\cup(S-R),$$

也就是说，S' 是 S 中把 R 挖去换成 R' 的集合. 因为 $S\cap S'=S-R$，我们命 $S-R$ 中元与它自身对应，R 中元与 R' 中元的对应关系不变(根据假设 R 与 R' 同构). 我们就得到 S 射到 S' 的可逆映射. 假定这映射用 $a\to a'$ 表示，这时，我们规定 S' 的结合法是

$$a'+b'=(a+b)',a'b'=(ab)',$$

显然 S' 是环，并且其中 R' 的结合法与原来的一样，没有变动，因此 S' 是 R' 的扩张环. 再我们容易知道 $a\to a'$ 就是 S 到 S' 上的同构，所以 $S\simeq S'$，因此定理成立.

同 §2.5 习题 9 一样，关于环我们常常引用与同态类似的另一种映射. 假定 σ 是环 R 射到 R' 上的映射，并且对于 R 中任意元 a,b，

---

*) 其实这条件可以不要，因为如果有公共元，做一次挖补就行了.

$$\sigma(a+b)=\sigma(a)+\sigma(b),\sigma(ab)=\sigma(b)\sigma(a),$$

那么 σ 叫做 R 到 R' 上的逆同态，R 叫做与 R' 逆同态. 当 σ 是单射时，σ 就叫做 R 到 R' 的逆同构，这时 R' 又叫做 R 的逆环. 显然，环与它的逆环的逆环同构. 假如环是交换的，那么逆同态就是同态，因此对于交换环，我们就不需要逆同态这个名词了.

1949 年华罗庚发表了下面的定理，在这里我们只叙述这定理，它的证明我们就不谈了[12].

假定 σ 是环 R 射到 R' 的映射，它使 R 中两元的和与这两元在 R' 中象的和对应，两元的积与这两元的象的积对应，那么 R 中两元在 R' 中象的积的顺序只有两种可能，一是都与它们的象源的积的顺序一致，一是都与象源的积的顺序相反. 不存在某些两元的象的积的顺序与象源的积的顺序一致，而另一些则相反，也就是说，这时 σ 是 R 到 R' 上的同态或者是逆同态.

习 题 3.3

1. 假如 R 是环，S 是非空集合，并且有闭合的加法与乘法，如果 σ 是 R 射到 S 上的映射，它保持元素间的和及积的关系，那么 S 也是环(参看 §2.5 定理 1). 又假如 R 是体，S 是否仍然是体?

2. 试证所有整数组成的加群与所有偶数组成的加群同构，但整数环不与偶数环同构.

3. 试证体的乘群不与它的加群同构.

4. 高斯数体的自同构只有恒等同构及 $a+bi\to a-bi$ 两个.

5. 有理数加群的自同态环与有理数域同构.

6. 试证所有形如

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix},a,b,c,d \text{ 都是实数}$$

的 2 阶矩阵组成一个与实四元数体同构的体.

7. 假定 K 是实四元数体，$\alpha=ea+bi+cj+dk$，$\alpha'=ae-bi-cj-dk$，试证 $\alpha\to\alpha'$ 是 K 的自逆同构.

8. 假定环 R 有单位元，$\tau_a(r)=ra$，试证所有 τ_a 形成与 R 逆同构的环.

9. 环的加群如果是循环群，叫做循环环[13]. 试证 n 阶循环环互不同构的个数等于 n 的正约数的个数.

10. 任意两个有单位元的 m 元环，如果 m 没有平方数因子，试证这两个环同构.

§ 3.4 分 式 域

环所以不能成为体，是因为它的元不一定都有逆元. 我们可否把这些逆元以及与逆元的乘积都添入使它成为体？也就是说，环是否可以扩张成为体？ 或者说一个环能否嵌入于一体？

我们知道，整数集 Z 只成为整环，它不能成为体，因为它的元除 1 及 −1 两数外，都没有逆元. 如果我们把这些逆元以及逆元的乘积也就是把所有由整数做成的分式添入，那就成为有理数域 Q. 现在我们仿照这方法，从交换环 R 做出这些逆元，也就是这些"分式"，添加于 R 使它成为包含 R 的域，这就是说，对于一个交换环，我们可以做一个域把所给的环嵌入. 我们分两步来进行. 首先假设已知有一个包含 R 的体 K，在这 K 中如何去找这些分式或者商，使它们成为包含 R 的域，其次，在一般情况下，假定包含 R 的体不是已知，如何去从一个交换环做出分式成为包含它的域.

我们知道，假如 a,b 是体中非零的元，如果 $ab=ba$，那么 $ab^{-1}=b^{-1}a$，这就是说，b 左除 a 与 b 右除 a 结果是一致的. 因此我们就简单地叫它做 b 除 a 的分式用 $\frac{a}{b}$ 来表示，即

$$\frac{a}{b}=ab^{-1}=b^{-1}a.$$

定理 1 假设 K 是包含交换环 R 的体，那么 K 中所有的分式*) $\frac{a}{b}$，$b\neq 0$，$a,b\in R$，形成一个包含 R 的域 F，这 F 叫做 R 的分

*) b 虽然在 R 中，但 b^{-1} 不一定在 R 中，因此 $ab^{-1}=b^{-1}a$ 也不一定在 R 中.

式域.

证明 首先我们容易得知,对于这些分式,下面的计算法则都能够成立.

$1°\quad \frac{a}{b}=\frac{c}{d}$,当 $ad=bc$, $\qquad 2°\quad \frac{ca}{cb}=\frac{ac}{bc}=\frac{a}{b}$,

$3°\quad \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $\qquad 4°\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$.

这是因为,如果 $\frac{a}{b}=\frac{c}{d}$,即 $b^{-1}a=cd^{-1}$,那么 $ad=bc$,所以1°成立. 2°可由1°直接推得,再因为

$$\frac{ad+bc}{bd}=(bd)^{-1}(ad+bc)=(bd)^{-1}(ad)+(bd)^{-1}(bc)$$

$$=\frac{ad}{bd}+\frac{bc}{bd}=\frac{a}{b}+\frac{c}{d},$$

$$\frac{a}{b}\cdot\frac{c}{d}=b^{-1}ad^{-1}c=b^{-1}d^{-1}ac=(bd)^{-1}\cdot ac=\frac{ac}{bd},$$

所以3°,4°都成立.

因为分式 $\frac{0}{a}=0$,所以0也是分式. 再因为

$$\frac{a}{b}+\frac{-a}{b}=\frac{a+(-a)}{b}=\frac{0}{b}=0,$$

所以 $\frac{a}{b}$ 的负元是分式 $\frac{-a}{b}$. 因此所有这些分式,也就是 F,成为加群.

又因为 $\frac{a}{a}=e$(K 的单位元),所以 e 也是分式. 再因为

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=e \qquad (a,b\neq 0),$$

所以 $\frac{a}{b}$ 的逆元是分式 $\frac{b}{a}$,于是 F 对乘法也成群,因此 F 是体,显然它是域.

最后,对于 R 中任意元 a,我们有 $\frac{ab}{b}=a$,这里 b 是 R 中任意非零的元,所以 $F\supseteq R$,因此定理得证.

从上面的证明我们可以看出两件事情:第一,在我们的证明

中，只要 R 能够嵌入一个体中，就可以证明 R 的分式域 F 存在.并且两个分式的相等以及它们的加法，乘法都完全是由 R 的结合法唯一确定，所以分式域 F 的构造完全是由 R 确定，因此如果 R 能够嵌入两个体中，那么得到的两个分式域就同构，也就是说，R 的分式域都同构.我们更可以知道，同构的环的分式域也是同构的.第二，任一体 K，如果包含 R，也就包含 R 的分式域 F.因此 F 是包含 R 的最小域.譬如，有理数域 Q 是整数环 Z 的分式域，它是包含 Z 的最小域.

现在我们来讨论一般交换环 R(包含它的体不是已知)是否有分式域？假如有，当然也是由 R 中元的分式形成的域，但是这时分式是表示什么？我们如何来认识？

我们知道域中没有零因子，如果 R 有分式域 F，因为 R 是 F 的子集，所以 R 也不能有零因子，也就是说 R 必须是整环.这是必要条件，下面我们来证明它也是充分条件.

定理 2 交换环 R 有分式域的必要充分条件是 R 为整环.

证明 定理的必要性已如上述，现在只证明充分性.

先考虑 R 中所有元素对 (a,b)，$b\neq 0$.两个元素对 (a,b)，(c,d)，当 $ad=bc$ 时，我们用记号

$$(a,b)\sim(c,d)$$

表示.显然，这个关系满足自反律、对称律，并且它也满足传递律.这是因为，由 $(a,b)\sim(c,d)$、$(c,d)\sim(e,f)$，就可以得到

$$ad=bc、cf=de,$$

因此

$$adf=bcf=bde.$$

但 R 是整环，所以 $af=be$，即 $(a,b)\sim(e,f)$.于是这关系是一个等价关系.由§1.2定理，我们可以根据这关系把所有这些元素对组成的集分成为若干类，使相互等价的同在一类.(a,b) 所在的类用 $\frac{a}{b}$ 表示.下面我们来讨论由所有这些类组成的集 F.

显然，$\frac{a}{b}=\frac{c}{d}$的必要充分条件是$(a,b)\sim(c,d)$，也就是$ad=bc$. 因此，定理1证明中的计算法则1°，2°这时都同样成立.

我们再用前面的计算法则3°，4°来做这些类的加法、乘法的定义，也就是说，我们规定

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

这个规定是唯一的. 首先因为$b\neq 0$，$d\neq 0$，R又没有零因子，所以$bd\neq 0$，因此$\frac{ad+bc}{bd}$及$\frac{ac}{bd}$都有意义，也就是说，这两个类的确都是F中元. 其次，如果$\frac{a'}{b'}=\frac{a}{b}$，$\frac{c'}{d'}=\frac{c}{d}$，我们很容易证明

$$\frac{a'd'+b'c'}{b'd'}=\frac{ad+bc}{bd},\quad \frac{a'c'}{b'd'}=\frac{ac}{bd},$$

因此$\frac{a}{b}+\frac{c}{d}$及$\frac{a}{b}\cdot\frac{c}{d}$的结果与在类$\frac{a}{b}$，$\frac{c}{d}$中选取的元素对$(a,b)$、$(c,d)$没有关系，也就是说，这些类的和及积是唯一的. 再我们这样定义的加法及乘法显然都满足交换律，并且关于加法及乘法的结合律都是成立的. 又因为

$$\left(\frac{a}{b}+\frac{c}{d}\right)\frac{e}{f}=\frac{ad+bc}{bd}\cdot\frac{e}{f}=\frac{(ad+bc)e}{bdf},$$

$$\begin{aligned}\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}&=\frac{ae}{bf}+\frac{ce}{df}=\frac{adef+bcef}{bdf^2}\\&=\frac{(ad+bc)ef}{bdf^2}=\frac{(ad+bc)e}{bdf},\end{aligned}$$

所以分配律也成立.

所有元素对$(0,a)$，$(0,b)$，$\cdots(a,b,\cdots\neq 0)$都属于同一类$\frac{0}{a}$，它是加法的单位元，也就是说，它是零元，这是因为

$$\frac{0}{a}+\frac{c}{d}=\frac{0d+ac}{ad}=\frac{ac}{ad}=\frac{c}{d}.$$

类$\frac{-a}{b}$是$\frac{a}{b}$的负元，这是因为

$$\frac{a}{b}+\frac{-a}{b}+\frac{a-a}{b}=\frac{0}{b}.$$

所有元素对(a,a)，(b,b)，$\cdots(a,b,\cdots\neq 0)$都属于同一类$\frac{a}{a}$，它是乘法的单位元，这是因为

$$\frac{a}{a}\cdot\frac{c}{d}=\frac{ac}{ad}=\frac{c}{d},$$

类$\frac{a}{b}(\neq 0)$的逆是$\frac{b}{a}$，这是因为

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ab},$$

因此，我们证明了F成为域.

下面我们证明R与F的一个子环同构. 我们来考虑F中所有形如$\frac{aq}{q}$，$q\neq 0$的元集合S. 因为$\frac{aq}{q}=\frac{aq'}{q'}=\frac{aq''}{q''}$，所以不妨固定一个$q$，因此$S$是所有形如$\frac{aq}{q}$，$a\in R$，的元组成的集，显然它是$F$的子环. 假如命$R$中元$a$与$S$中元$\frac{aq}{q}$对应，即$a\to\frac{aq}{q}$，那么这对应是$R$射到$S$的双射，这是因为，从

$$\frac{aq}{q}=\frac{bq}{q},q\neq 0,$$

就得到

$$aq^2=bq^2,$$

但R没有零因子，所以$q^2\neq 0$，因此$a=b$. 再从

$$a\to\frac{aq}{q},b\to\frac{bq}{q},$$

我们就有

$$a+b\to\frac{(a+b)q}{q}=\frac{aq+bq}{q}=\frac{aq}{q}+\frac{bq}{q},$$

$$a\cdot b\to\frac{abq}{q}=\frac{abqq}{qq}=\frac{aq\cdot bq}{q\cdot q}=\frac{aq}{q}\cdot\frac{bq}{q},$$

所以这映射是R到S的同构，即$R\simeq S$. 因此S也是环.

根据§3.3定理4，我们可以把R看成F的一部分，也就是说$F\supseteq R$，因此F就是R中所有元的分式形成的域，所以F是R的分式域. 于是定理得证.

上面虽然是定理2的充分性证明，但同时也是把一个整环嵌入一个域的方法，因此对任一整环我们都可以作出它的分式域.

假如 R 只是交换环，不一定是无零因子，S 是 R 中所有非零因子的集合，因为 ab 是零因子时，a,b 中最少有一是零因子，所以 S 是半群. 同上面一样，R 能够嵌入由所有分式 $\frac{r}{s}$，$r\in R$，$s\in S$ 形成的环中，这环叫做 R 的**分式环**. 显然它有单位元，并且 S 中任意非零元在分式环中都有逆元.

要注意的是，非交换无零因子环一般是没有分式域的，也就是说它不能够嵌入于域. 1936 年马尔采夫(А. И. Мальцев)曾给出了一个例子[14]来说明这问题，但是也有有分式体的，譬如，非交换主理想环(§3.9)就有分式体[15]，1931 年渥尔(O. Ore，1899～1968)曾证明[16]一般非交换无零因子环，假如满足任意两元 a,b 都有左(右)公倍元 $a'b=b'a\neq 0$($ba'=ab'\neq 0$)的条件，它就有分式体，也就是说，它能够嵌入于体. 这些我们都不详细证明了.

习 题 3.4

1. 假设 p 是质数，试证所有形如 $\frac{m}{n}$，$(n,p)=1$，的有理数集成为整环，并求它的分式域.

2. 试证任意适合消去律的交换半群能够嵌入于群.

3. 假定 R 是没有单位元的环，Z 是整数环，试证所有形如 (a,m)，$a\in R$，$m\in Z$，的元适合下列关系：

1) $(a,m)=(b,n)$，当 $a=b$，$m=n$；

2) $(a,m)+(b,n)=(a+b,m+n)$；

3) $(a,m)\cdot(b,n)=(ab+na+mb,m\cdot n)$.

时，成为一个有单位元的环，单位元是 $(0,1)$，我们用 (R,Z) 表示. 它包含 R 及 Z. 于是任意没有单位元的环能够嵌入一个有单位元的环，也就是说，任意没有单位元的环能够看成为有单位元的环的子环.

§3.5 多项式环

我们已经知道环的一般概念，这节介绍一种特殊的环，它的结

合法是具体的，并且它在数学上也占极重要地位.

普通代数中讨论的多项式，它的系数都是实数或复数，现在我们把这个概念推广到一般情形.

定义 假定 R 是有单位元 1 的环，x 是记号，也就是未定元，那么形如下面的表达式

(1) $$f(x)=\sum a_i x^i = a_0x^0+a_1x+\cdots+a_nx^n, a_i\in R,$$

叫做环 R 上 x 的**多项式**，或者简称为 x 的多项式，a_i 叫做它的**系数**.

首先我们规定，在 $f(x)=\sum a_ix^i$ 中，当 $a_j=0$ 时 a_jx^j 就可以略去不写，也就是说，在一个多项式中，我们可以任意增加或减少系数是零的项. 再我们来规定两个多项式的相等以及它们的加法、乘法，这些也正是普通代数中多项式的计算法则：

(2) $$\sum a_ix^i=\sum b_ix^i，当\ a_i=b_i,$$

(3) $$\sum a_ix^i+\sum b_ix^i=\sum(a_i+b_i)x^i,$$

(4) $$\sum a_kx^k\cdot\sum b_lx^l=\sum c_ix^i, c_i=\sum_{k+l=i}a_kb_l.$$

在(2)，(3)两式中，如果两个多项式的项数不同，我们可以用系数是零的项来填补.

由(4)定义的乘法非常容易记忆，只要把多项式中形式的加法与乘法假定分配律成立而展开就得了. 但要注意的是 a_k, b_l 的顺序不能颠倒，因为 R 不一定是交换环.

我们很容易证明，R 上所有 x 的多项式形成一个环，叫做**添加未定元 x 于 R 形成的环**，或者叫做 R 上 x 的**多项式环**，或简称 x 的**多项式环**，用记号 $R[x]$ 表示. 这时系数都是零的多项式是它的零元，多项式 $\sum a_ix^i$ 的负元是

$$\sum(-a_i)x^i=-\sum a_ix^i.$$

系数 $a_i\neq 0$ 的 i 中最大数，叫做多项式的**次数**. 譬如在(1)中，如果 $a_n\neq 0$，那么 $f(x)$ 就是 n 次的，这时，a_nx^n 就叫做 $f(x)$ 的**首项**. 一个零次多项式是如 a_0x^0，$a_0\neq 0$，形状的. 如果多项式的所有系数都是

零，那么它就没有次数了. 因此 $R[x]$ 的零元就是没有次数的多项式.

$R[x]$ 中所有零次多项式及零元成为一个子环，假如我们把 R 中元 a 与多项式 ax^0 对应，那么这对应就是 R 到这子环的同构，因此 R 与这子环同构. 由 §3.3 定理 4，我们可以把 R 看成 $R[x]$ 的子环，也就是说，把 a 看成 ax^0，于是 $R[x]$ 的零元就是 R 的零元，零次多项式就是 R 中非零元，所以我们又可以把(1)改写成

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n.$$

再假如我们把多项式 $1x$ 改写成 x，即 $1x=x$，那么 x 就是 $R[x]$ 中元，因此 $R[x]$ 是包含环 R 及未定元 x 的环，于是 ax 就是 $R[x]$ 中元 a,x 的乘积.

假如 Z 是环 R 的中心，那么 $Z[x]$ 就是 $R[x]$ 的中心[10].

我们知道 $R[x]$ 是 R 的扩张环，当然 $R[x]$ 不具备 R 的一切性质，但它也保持 R 的某些性质. 显然，R 的单位元 1 就是 $R[x]$ 的单位元，假如 R 是交换环，那么 $R[x]$ 也是交换环，此外我们还有

定理 1 假定 R 是整环，那么 $R[x]$ 也是整环.

证明 假设 $f(x)=a_0+a_1x+\cdots+a_nx^n, a_n\neq 0$,

$$g(x)=b_0+b_1x+\cdots+b_mx^m, b_m\neq 0,$$

那么

$$f(x)g(x)=a_0b_0+\cdots+a_nb_mx^{n+m},$$

但 R 是无零因子环，所以 $a_nb_m\neq 0$，这就是说，$R[x]$ 没有非零的零因子，于是 $R[x]$ 是整环，因此定理成立.

譬如，整数环 Z 的多项式环 $Z[x]$ 是整环，这时多项式就是普通整系数多项式.

由上面给的证明，我们又知道，假如 R 是无零因子环，$f(x)$，$g(x)$ 是 $R[x]$ 中次数分别为 n,m 的多项式，那么 $f(x)\cdot g(x)$ 就是 $R[x]$ 中次数是 $n+m$ 的多项式. 当 R 有零因子时，$R[x]$ 显然也有零因子. 关于 $R[x]$ 的零因子，1942 年麦珂(N. H. McCoy，1905～)曾经证明这样一个性质[17]，假定 R 是交换环，那么 $f(x)$ 是 $R[x]$ 的零因子的必要充分条件是 R 中有一非零元 a，使得 $af(x)=0$.

1954 年斯谷脱(W. R. Scott, 1919～)用反证法来证明,非常简单,读者可参考文献[18]. 但要注意的是当 R 不是交换环时,这定理是不成立的[19].

现在我们来讨论未定元 x 取"值"的问题.

我们把 R 的扩张环 R' 中一元 a 来代替多项式(1)中未定元,就得到 $x=a$ 时 $f(x)$ 的值

$$f(a)=a_0+a_1a+\cdots+a_na^n,$$

它当然仍然是 R' 中一元. 假如 $f(x)=\sum a_ix^i, g(x)=\sum b_ix^i$, 那么它们的和及积

$$s(x)=f(x)+g(x), p(x)=f(x)g(x)$$

当 $x=a$ 时的值就分別是 $s(a), p(a)$. 我们要注意的是, $s(a)$ 与 $f(a)+g(a)$ 的意义不同, $p(a)$ 与 $f(a)g(a)$ 的意义也不同. 这是因为 $f(a)$、$g(a)$ 是 R' 中元, $f(x)$、$g(x)$ 是 $R'[x]$ 中元, $s(a), p(a)$ 是先结合而后代入的结果,而 $f(a)+g(a), f(a)g(a)$ 则是先代入后结合的结果,两者可能不一致. 但

$$\begin{aligned} s(a) &= (a_0+b_0)+(a_1+b_1)a+\cdots+(a_n+b_n)a^n \\ &= (a_0+a_1a+\cdots+a_na^n)+(b_0+b_1a+\cdots b_na^n) \\ &= f(a)+g(a), \end{aligned}$$

而

$$p(a)=a_0b_0+(a_0b_1+a_1b_0)a+\cdots+a_nb_ma^{n+m}$$

却不一定与 $f(a)g(a)$ 相等,因为这时 a 不一定与 b_i 都能够交换. 为了避免这种困难,当我们用 R' 中元 a 来代替多项式 $f(x)$ 的未定元 x 时,我们要求 a 与 R 中任意元都可交换,这样也就有 $p(a)=f(a)g(a)$ 了. 如果 R' 是交换环,那么 R' 中的任意元都可以代入 $f(x)$ 中. 假如 $f(a)=0$, 那么 a 叫做 $f(x)$ 的零点,有时也叫做 $f(x)$ 的根. 以后我们说 a 是 $f(x)$ 的零点或根,就意味着 a 是 R 的扩张环中的元,并且它与 R 中的任意元都能够交换.

下面,我们来讨论关于 $R[x]$ 的欧几里得(Euclid)法式.

假定

$$f(x)=a_0+a_1x+\cdots+a_nx^n, a_n\neq 0,$$

是$R[x]$中任一多项式，又

$$g(x)=b_0+b_1x+\cdots+b_{m-1}x^{m-1}+x^m$$

是$R[x]$中另一多项式，只要求它的首项系数是1，那么在$R[x]$中就有两个满足

(5) $$f(x)=q(x)g(x)+r(x)$$

的多项式$q(x)$，$r(x)$，这时$q(x)$叫做$g(x)$除$f(x)$的**右商**，$r(x)$是次数小于m的多项式或零元，叫做$g(x)$除$f(x)$的**右余式**. 假如$g(x)$的次数大于$f(x)$的次数，我们取$q(x)=0$，$r(x)=f(x)$，那么(5)式就显然成立；假如$g(x)$的次数不大于$f(x)$的次数，我们可以自$f(x)$减去$a_nx^{n-m}g(x)$，在得到的多项式

$$f(x)-a_nx^{n-m}g(x)=r_1(x)$$

中，x^n的系数是零元，所以它的次数小于n. 如果$r_1(x)$的次数大于m，我们可以再用同样的方法，自$r_1(x)$中减去$g(x)$的倍数，这样继续下去，在有穷回后，一定可以得到一个多项式$r(x)$，它的次数小于m或者是$r(x)=0$，因此(5)式成立.

如果R是体，$g(x)$的首项系数就可以是任意元$b_m\neq 0$而不必要求是1，因为对于$\frac{1}{b_m}g(x)$，我们有

$$f(x)=q(x)\cdot\frac{1}{b_m}g(x)+r(x)=q(x)\frac{1}{b_m}\cdot g(x)+r(x),$$

把$q(x)\frac{1}{b_m}$看成(5)式中的$q(x)$，那么(5)式就显然成立.

同上面一样，在$R[x]$中有满足

(6) $$f(x)=g(x)q_0(x)+r_0(x)$$

的多项式$q_0(x)$，$r_0(x)$，这时$q_0(x)$叫$g(x)$除$f(x)$的**左商**，$r_0(x)$是次数小于m的多项式或是零元，叫$g(x)$除$f(x)$的**左余式**. 当R是交换环时，右商也是左商，右余式也是左余式，这时我们就简称为**商**及**余式**. 当R是无零因子环时，(5)式中的$q(x)$，$r(x)$及(6)式中的$q_0(x)$，$r_0(x)$都是唯一的. 上面(5)，(6)两式，我们叫做欧几里

得法式，或简单地叫做欧氏法式.

同普通代数中讨论的一样，当R是域时，$R[x]$中多项式$f(x)$，$g(x)$的最大公因式$d(x)$可以引用欧氏法式求得，并且

$$d(x)=u(x)f(x)+v(x)g(x),u(x),v(x)\in R[x],$$

因此$d(x)$是$R[x]$中元.

假定α是R的扩张环中元，如果α是$R[x]$中非零的多项式的零点，那么α就叫做R的**代数元**. 如果α不是$R[x]$中非零的多项式的零点，也就是说，也不适合$R[x]$中任意非零的多项式，那么α就叫做R的**超越元**. 我们容易证明，$R[x]$射到$R[\alpha]$上的映射

$$\sum a_i x^i \to \sum a_i \alpha^i,$$

当α是R的代数元时，它是同态；当α是R的超越元时，它是同构. 因此上面所说的未定元x就是R的超越元.

我们知道$R[x]$的单位元就是R的单位元，也就是说，$R[x]$也是有单位元的环，因此我们又可以自$R[x]$再添加一个未定元y，得到环$R[x][y]$. 一般，我们可以在R上陆续添加n个未定元x_1，$x_2,\cdots,x_n$，得到$R[x_1][x_2]\cdots[x_n]$. 如果我们假定这些未定元能够相互交换，那么在R上添加这些元时，就与添加的顺序无关，这时就写成$R[x_1,x_2,\cdots,x_n]$，叫做**添加n个未定元$x_1,x_2,\cdots,x_n$于R形成的环**，或者叫做**n个未定元的多项式环**，其中的多项式可以写成

$$f(x_1,x_2,\cdots,x_n)=\sum a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}.$$

同一个未定元的情形一样，我们容易证明，假如R是交换环，那么$R[x_1,x_2,\cdots,x_n]$也是交换环，若R是整环，则$R[x_1,x_2,\cdots,x_n]$也是整环，R或它的扩张环中与R的所有元能够交换的元可以代入$R[x_1,x_2,\cdots,x_n]$中任一多项式而得出它的值. 当R是交换环时，如果$f(x_1,x_2,\cdots,x_n)$是$R[x_1,x_2,\cdots,x_n]$的零因子，那么R中也有非零的元a，使$af(x_1,x_2,\cdots,x_n)=0$[20].

同环R上x的多项式类似，表达式$\sum\limits_{i=0}^{\infty}a_i x^i$，$a_i\in R$，叫做$R$上

形式的 x 的幂级数. 我们根据普通幂级数的相等,相加及相乘规定它们的相等及加法、乘法. 显然 R 上所有 x 的幂级数形成的环,叫做 R 上 x 的幂级数环,或简称幂级数环,用 $R[[x]]$ 表示. 同上面一样,R 的单位元 1 也是 $R[[x]]$ 的单位元,R 是 $R[[x]]$ 的子环,下面性质是多项式环不具备的.

定理 2 $f=\sum_{i=0}^{\infty}a_ix^i$ 是 $R[[x]]$ 中可逆元的必要充分条件是 a_0 是 R 中可逆元.

证明 假定 f 是可逆元,那就有 $g=\sum_{i=0}^{\infty}b_ix^i$ 使 $fg=gf=1$,根据乘法规则,我们得 $a_0b_0=b_0a_0=1$,所以 a_0 是可逆元.

反之,若 a_0 是可逆元,要由 $fg=1$ 来构作 g. 由乘法规则有

$$a_0b_0=1, a_0b_1+a_1b_0=0, \cdots, a_0b_n+a_1b_{n-1}+\cdots+a_nb_0=0, \cdots.$$

显然 $b_0=a_0^{-1}$, $b_1=a_0^{-1}(-a_1b_0)=a_0^{-1}(-a_1a_0^{-1})$. 若 $b_0, \cdots, b_{n-1}$ 已由诸 a_i 决定,则因 $b_n=a_0^{-1}(-a_1b_{n-1}-\cdots-a_nb_0)$,$b_n$ 亦可由诸 a_i 决定. 因此,由归纳法,$b_0, b_1, \cdots, b_n, \cdots$ 中的任何一个都可由诸 a_i 决定. 即,$R[[x]]$ 中有 g,使 $fg=1$. 仿之,$R[[x]]$ 中有 h,使 $hf=1$. 注意到 $h=h1=h(fg)=(hf)g=1g=g$,推知 f 为 $R[[x]]$ 的可逆元.

习 题 3.5

1. $R[x]$ 中一个 m 次多项式与一个 n 次多项式的乘积是否是一个 $m+n$ 次多项式,为什么?

2. 假定 R 是有单位元的整环,试证 $R[x]$ 的可逆元是 R 的可逆元.

3. 假定 $f(x)$ 是 $R[x]$ 中多项式,α 是 R 的扩张环中元,试证"剩余定理"

$$f(x)=q(x)(x-\alpha)+f(\alpha).$$

4. 假定 $Z_2[x]$ 中多项式

$$f(x)=\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}2&0\\2&0\end{pmatrix}x^2, g(x)=\begin{pmatrix}1&2\\-2&1\end{pmatrix}+\begin{pmatrix}1&0\\0&1\end{pmatrix}x,$$

试求 $g(x)$ 除 $f(x)$ 的右商 $q(x)$,右余式 $r(x)$ 及左商 $q_0(x)$,左余式 $r_0(x)$.

5. 假如 R 是有单位元的环，试证 $R[x]$ 的中心

$$Z(R[x])=Z(R)[x].$$

6. 假定 $x_1,x_2,\cdots,x_n,\cdots$ 是无穷多个未定元，R 是环，试定义多项式环 $R[x_1,x_2,\cdots,x_n,\cdots]$，其中多项式只包含有穷个未定元.

§3.6 理 想

在§2.5中，我们得知由正规子群可以做商群，环可以看成加群，所以由子环可以做同余加群. 但有的同余加群又能够成为环，譬如§3.1中给出的 $\overline{Z}_n=Z-(n)$ 就是环. 一般来说，么样的子环，它的同余加群才能成为环？这种子环要满足什么条件？这样就引进了理想的概念.

我们知道，环 R 关于它的子环 N 的同余加群 $\overline{R}=R-N$ 是所有同余类 $a+N=\bar{a}$ 的集合，因为当 $a\equiv a'(N)$，$b\equiv b'(N)$ 时，$a+b\equiv a'+b'(N)$，所以我们可以规定 $\bar{a}$，$\bar{b}$ 的和为 $\bar{a}+\bar{b}=\overline{a+b}$. 要希望 $\overline{R}$ 成环，首先还要规定 $\bar{a}$，$\bar{b}$ 的积. 同§3.1中 $\overline{Z}_n$ 的情形一样，我们来考虑同余类 $\bar{a}$ 中任意元与同余类 $\bar{b}$ 中任意元的乘积是否与 ab 同在一同余类. 也就是说，由 $a\equiv a'(N)$，$b\equiv b'(N)$，我们能否得到 $ab\equiv a'b'(N)$. 假如能够，那么对于 N 中任意元 n_1,n_2，我们有

$$(a+n_1)(b+n_2)=ab+an_2+n_1b+n_1n_2\equiv ab(N),$$

也就是

$$an_2+n_1b\equiv 0(N).$$

当 $n_1=0$ 时，$an_2\equiv 0(N)$；当 $n_2=0$ 时，$n_1b\equiv 0(N)$，因此对于 R 中任意元 r，我们有

$$(1)\qquad rN\subseteq N,\ Nr\subseteq N.$$

反之，假如子环 N 具有上面性质(1)，显然由

$$a\equiv a'(N),b\equiv b'(N),$$

我们就得到 $ab\equiv a'b'(N)$. 但一般子环无此性质. 故而引进

定义 假定 R 是环，N 是它的子环，如果对于 $a\in N$，$r\in R$，我

们就有 $ra(ar)\in N$，那么 N 就叫做 R 的左(右)理想. 假如 N 是 R 的左理想同时又是 R 的右理想，也就是说，当 $a\in N, r\in R$ 时，$ra\in N, ar\in N$，我们就叫 N 为 R 的理想.

显然，N 对乘法的闭合性已包含在条件(1)中，所以 R 的子集 N 成为左(右)理想的条件，只要它是加群，并且满足条件：当 $a\in N, r\in R$ 时，$ra(ar)\in N$ 就行了.

假如 R 是交换环，那么左、右理想及理想的意义是一致的，因此交换环中，理想就不必区别左与右了.

于是 R 中理想 N 的同余类 $\bar{a}, \bar{b}$ 的积，我们可以规定为

$$\bar{a}\cdot\bar{b}=\overline{ab}.$$

显然 $\bar{R}=R-N$ 对这样规定的乘法是闭合的. 再因为 R 中元满足结合律、分配律，所以 N 的同余类也同样满足结合律、分配律. 因此 $\bar{R}$ 成环，这环我们叫做 R 关于 N 的同余环. 我们容易知道，$\bar{R}$ 的零元就是 R 的零元 0 所在的同余类 $\bar{0}$，也就是 N 自身. 当 R 有单位元 e 时，e 所在的同余类 $\bar{e}$，就是 $\bar{R}$ 的单位元. 假如 R 是交换环，那么同余环 $\bar{R}$ 也是交换的.

要注意的是，上面因为我们希望 N 的两个同余类的积仍然是 N 的一个同余类，所以要求 N 是理想，这与 § 2.3 中陪集 $aHbH$ 的积是陪集 abH 时，要求 H 是正规子群的情形一样.

上面介绍了理想及同余环的概念，现在我们来讨论理想

显然，环自身是它的理想，叫做单位理想. 只一个零元也形成理想，叫做零理想. 由定义我们容易得知，偶数环 $2Z$ 是整数环 Z 的理想. 在全矩阵环 Z_2 中，所有形如$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$的矩阵成为它的左理想而不是右理想. 所有形如$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$的矩阵成为它的右理想，但不是左理想. 所有形如$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$的矩阵成为 Z_2 的子环，不是左理想也不是右理想. 环的中心不是理想.

假定环 R 有单位元 e，N 是它的左(右)理想，如果 $e\in N$，那么

$r=re(er)\in N, r\in R$，因此 $R\subseteq N$，所以 $N=R$. 这就是说有单位元环的真左(右)理想不含单位元.

同群的情况一样，一个环的任意多个左(右)理想的交集仍然是一个左(右)理想，但任意两个左(右)理想的并集却不一定是左(右)理想

假定环 A 与环 B 同态(不一定在上)，A 的理想在 B 的象不一定是 B 的理想，但 B 的理想在 A 的完全象源是 A 的理想.

下面主要是理想的形成.

假定 R 是交换环，a 是 R 中一元，那么 R 中所有形如

(2) $$ra+na, r\in R, \quad n \text{ 是整数或零}^{*)}$$

的元成为一个理想，叫做由元 a **生成的理想**，用 $\langle a\rangle$ 或 (a) 表示，这是因为

$$(r_1a+n_1a)-(r_2a+n_2a)=(r_1-r_2)a+(n_1-n_2)a\in(a),$$

$$r_1(ra+na)=r_1ra+nr_1a=(r_1r+nr_1)a\in(a),$$

所以 (a) 是理想.

不难看出，任意包含 a 的理想都包含 (a)，因此，我们也说 (a) 是包含 a 的最小理想. 又因为任意多个理想的交集仍然是一个理想，所以 (a) 也是所有包含 a 的理想的交集.

如果 R 又有单位元 e，那么 $na=(ne)a$，于是(2)可以简写成

$$(r+ne)a=r'a, r'\in R,$$

因此，这时 (a) 是由 a 的一切倍元 ra 组成的. 譬如在整数环 Z 中理想 (m) 就是由 m 的一切倍数组成的. 假如 a 是幂等元，那么由 a 生成的理想 (a) 也是由 a 的倍元组成的. 要注意的是，由 a 生成的理

---

*) na 的意义是 n 个 a 相加，不是 R 中两个元的乘积，因为 n 是整数，不一定在 R 中，即令在 R 中，$n\cdot a$ 也不一定就是 na，但当 R 有单位元 e 时，na 确是 R 中两元的乘积，这是因为，

$$na=n(ea)=ea+\cdots+ea=(e+\cdots+e)a=ne\cdot a.$$

所以 $ra+na$ 不能写成 $(r+n)a$，因为这时 $r+n$ 不一定有意义.

想(a)包含a. 当R没有单位元时，所有形如$ra, r\in R$,的元虽然也成为理想，但一般它不包含a，因此它不一定是由a生成的理想(a). 譬如在$\overline{Z}_{12}$的子环$\overline{R}=\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\}$中，由$\overline{r4}, \overline{r}\in\overline{R}$,组成的理想包含$\overline{4}$，因此它是$(\overline{4})$，但由$\overline{r2}$组成的理想就不包含$\overline{2}$，因此它不是$(\overline{2})$

同样，我们又可以定义由交换环R中n个元$a_1, a_2, \cdots, a_n$生成的理想$\langle a_1, a_2, \cdots, a_n\rangle$，它是由所有形如

$$\sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{n} n_i a_i, r_i\in R, n_i \text{ 是整数或零},$$

的元组成的，$a_1, a_2, \cdots, a_n$叫做它的**生成元**. 如果R有单位元，那么，上式又可简写成$\sum_{i=1}^{n} r_i a_i$的形状.

假如R是非交换环，a是R中元，但不在中心$Z(R)$中，那么，由a生成的理想(a)是由所有象下面形状的元组成的：

$$r_1 a + a r_2 + \sum r_i a r_j + na, r_i\in R, n \text{ 是整数或零}.$$

当R有单位元时，上式可以简写成$\sum r_i a s_j$.

我们知道，环R的理想不一定是由一个元生成的，由一个元生或的理想，叫做**主理想**. 零理想是主理想，因为$0=(0)$；单位理想R，当R有单位元e的时候也是主理想，因为$R=(e)$. 多项式环$Z[x]$中所有常数项是偶数的多项式组成的理想是由$x, 2$生成的理想$\langle x, 2\rangle$，它不是主理想.

假定R是体，$N\neq 0$是R的左理想，a是N中非零的元，因为$a^{-1}a=e\in N$，所以$N=R$. 于是体除自身及零理想外，不含其他左理想及右理想.

反过来，假如环$R\neq 0$，除自身及零理想外，它不含其他左或右理想，我们命a是R中任一非零元，因为aR是R的右理想，所以$aR=R$或$aR=0$. 当R有单位元时，对于R中任意非零元a，我们都有$aR=R$，于是任意方程$ax=b$在R中都有解，因此R成体. 当R没有单位元时，R当然不能成体，因此R中有某非零元a，使aR

$=0$,于是对 R 中任意元 r,我们有 $ar=0$,这时

$$0,\pm a,\pm 2a,\cdots,\pm na,\cdots$$

显然成为 R 的右理想,因此它就是 R. 于是 R 是循环加群. 它只有元数是质数时才是单群,所以 R 是由质数 p 个元 $0,a,\cdots,(p-1)a$ 组成的环. 其中任意两元的乘积都是零,因此 R 是零环. 于是有

定理 1 假如环 $R(\neq 0)$除自身及零理想外,没有其他左或右理想,那么 R 有单位元时是体,没有单位元时是元数为质数的零环.

因此我们又得到

定理 2 有单位元的环,除自身及零理想外,没有其他左或右理想的必要充分条件是:它是体.

一个环至少有两个理想,一个是它自身——单位理想,一个是零理想. 只有这两个理想的环叫做**单纯环**,或简称**单环**. 显然体是单环,整数环不是单环. 由定理 1,我们又有

定理 3 交换单环($\neq 0$)是域或是元数为质数的零环.

单环不一定有单位元. 假如单环 R 有左单位元 e,那么 e 也是右单位元,因此是单位元,这是因为 $N=\{xe-x\mid x\in R\}$显然是 R 的理想,如果 $e\in N$,即 $e=ye-y$,那么 $e=0$. 但 e 是左单位元,所以 $ex=x=0$,即 $R=0$,此不可,所以 $N\subset R$. 因为 R 是单环,所以 $N=0$,于是 $xe=x$,因此 e 是单位元. 同样,单环如果有右单位元,那么它也有单位元. 再有穷单环可以由一个元或两个元生成[21].

假如 N 是环 R 的理想,那么 N_n 是全矩阵环 R_n 的理想,反过来基本上也成立,即假如 R 是有单位元的环,那么全矩阵环 R_n 的任意理想是全矩阵环 N_n,这里 N 是 R 的理想[22]. 要注意的是,这里有单位元是一个不可缺少的条件. 假如 R 没有单位元,这定理就不成立,后面§3.6的习题 2 是一个明显的例. 因此,如果 R 是有单位元的单环,那么 R_n 也是单环.

与汉弥尔顿群类似,有汉弥尔顿环. 一个环,如果它的任意子环都是理想,那么这环叫做**汉弥尔顿环**[23]. 譬如,整数环就是汉弥

尔顿环.

最后,我们来讨论理想与环的关系.正规子群是群的重要子群,理想是环的重要子环,理想在环中地位与正规子群在群中地位类似.下面定理更能说明这问题.这些定理及它的证法与§2.5中差不多,因此也可说是§2.5定理在环中的推广.

定理4 假定环R与环R'同态,R中元a在R'中的象是a',那么R'的零元$0'$的完全象源N是R的理想,叫做这同态的同态核,a'的完全象源是同余类$a+N$.

证明 首先,因为环的同态也是把环看成加群时的同态,所以N就是同态核.由§2.5定理2,我们得知N是加群,并且a'的完全象源是N的同余类$a+N$.

其次,当$a\in N$,$r\in R$时,我们有$a\to 0'$,$r\to r'$,于是

$$ra\to r'0'=0',\ ar\to 0'r'=0',$$

所以$ra,ar\in N$,这就是说N是R的理想,因此定理得证.

同群的情况一样,假如σ是同态核$\ker(R)$环R到环R'的同态,那么σ的象$\sigma(R)$是R'的子环,σ的同态核$\ker(R)$是R的子环,并且是理想.

假如两个环R,R'同态,即$R\sim R'$,同态核如果是零理想,那么$R\simeq R'$.如果是单位理想,那么R'是零.当R是单环时,因为R只有零理想及单位理想,所以这时同态核$N=R$或者$N=0$.因此R'是零或R与R'同构,这就是说,单环的同态象是单环或是零.假如R,R'都是体,因同态是R射到R'的映射,所以这时$N=0$,因此$R\simeq R'$.这就是§3.3中所说的体的同态是同构.

定理5 假定N是环R的理想,那么R与同余环$\overline{R}=R-N$同态,也就是说

$$R\sim\overline{R}$$

同态核就是N.

证明 我们把a与它所在的N的同余类$\overline{a}$对应,即$a\to\overline{a}$,那么这对应显然就是R到$\overline{R}$的满射,再因为

$$a+b \to \overline{a+b}=\bar{a}+\bar{b}, ab \to \overline{ab}=\bar{a}\bar{b},$$

所以 $R \sim \bar{R}$，因此定理得证.

定理 6 假定环 R 与环 R' 同态，同态核是 N，$\bar{R}=R-N$，那么

$$R' \simeq \bar{R}.$$

证明 因为 $R \sim R'$，假定这时的对应是 $a \to a'$，$\bar{a}$ 是 $\bar{R}$ 中 a 所在的同余类 $a+N$. 由上面定理 4，我们知道 $\bar{a}$ 是 a' 的完全象源，假如我们把 $\bar{a}$ 与 a' 对应，即 $\bar{a} \to a'$，显然这对应是 $\bar{R}$ 到 R' 的双射，并且

$$\bar{a}+\bar{b}=\overline{(a+b)} \to (a+b)'=a'+b',$$
$$\bar{a}\cdot\bar{b}=\overline{ab} \to (ab)'=a'b',$$

所以 $\bar{R} \simeq R'$，因此定理成立.

于是，任意同态象可以看成同余环，因此，理想能够决定环的所有同态，这是理想也是同余环的一个重要性质.

同 § 2.5 中一样，假如环 $R \sim R'$，N 是同态核，S 是 R 的子环，那么 S 在 R' 中的象 S' 也是 R' 的子环，并且 $S \sim S'$，同态核是 $S \cap N$，因此

$$S-(S \cap N) \simeq S'.$$

当 $S \supseteq N$ 时，

$$S-N \simeq S'.$$

习 题 3.6

1. 假设 R 是所有偶数形成的偶数环，试证所有形如 $4a(a \in R)$ 的数形成一个理想 A，它是否是主理想？假如 R 是整数环 Z，A 又怎样？

2. 假定 R 是偶数环，试证所有形如 $\begin{pmatrix} 2a & b \\ c & d \end{pmatrix}$ 的矩阵，这里 a,b,c,d 都是偶数，组成全矩阵环 R_2 的理想.

3. 试证同态 $R \sim R'$ 是同构的必要充分条件是它的同态核 $N=0$.

4. 假定 N 是环 R 的理想，如果 N 是正则理想(即对于 R 中任意元 a，R 中有元 e_1, e_2，使 $e_1 a \equiv a(N)$，$ae_2 \equiv a(N)$)，那么同余环 $R-N$ 有单位元.

5. $(x,2)$ 在 $Z[x]$ 中不是主理想，如何证明？

6. 假如 N 是有单位元环 R 的理想，那么

$$R[x]-N[x]\simeq(R-N)[x].$$

7. 所有形如 $a+bi$（a,b 是整数）的复数组成一个环，叫做高斯数环，试证 $Z[x]-(x^2+1)$ 与高斯数环同构，这里 Z 是整数环.

8. 假定 S 是环 R 的子环，N 是 R 的理想，并且 $S\cap N=0$，试证同余环 $R-N$ 中有与 S 同构的子环.

9. 假定 Z 是整数环，p 是质数，试证 $Z-(p^n)$ 中任意非零的理想包含 $\overline{p^{n-1}}$，也就是说，$Z-(p^n)$ 中所有非零理想的交异于零.

10. 假定 R 是元数大于 1 的整环，并且只包含有穷个理想，那么 R 是域.

11. 试证非幂零单环有单位元时中心是体，没有单位元时中心是零.

12. 假定 R 是单元零因子环，但不是体，L 是 R 的非零真左理想，那么 RL 是单无零因子环，并且没有单位元.

13. 一个非幂零环 R 是单环的必要充分条件是 $RxR=R$，这里 $0\neq x\in R$.

14. 假定 L 是有单位元环 R 的左理想，并且 $1+L=\{1+x|x\in L\}$ 中任意元都有左逆元，那么 $1+L$ 中任意元都是 R 的可逆元.

15. 假定 R 是单环，$R^2\neq 0$，e 是幂等元，那么 eRe 也是单环.

16. 假定 R 是环，如果其中任意元 a，R 中有元 a' 使 $a=aa'a$，那么 R 叫做正则环[24]. 显然体是正则环. 假定 a,b 是 R 中任意元，试证

$$1)\quad Ra=Re,\qquad 2)\quad Ra+Rb=Rf.$$

这里 e,f 都是幂等元.

§3.7 理想的运算

上节我们介绍了理想及它的性质，这节我们来介绍它们的运算：和、积及商.

假定 A,B 是环 R 的理想，那么所有形如

$$a+b,a\in A,b\in B$$

的元成为 R 的理想，叫做理想 A,B 的和，用 (A,B) 表示（§2.3）：

$$(A,B)=\{a+b|a\in A,b\in B\}.$$

显然，$(A,B)=(B,A)$，并且

$$((A,B),C)=(A,(B,C))=(A,B,C).$$

同和的情形不一样，所有形如

$$ab, a\in A, b\in B$$

的元不能成为 R 的理想，譬如 $A=\langle x,y\rangle$，$B=\langle x^2,y\rangle$ 是多项式环 $Z[x,y]$ 的理想，x^3，y^2 是形如 ab 的元，但 x^3-y^2 就不能写成 ab 的形状. 因此，我们来考虑所有有穷个元 ab 的和

$$\sum a_ib_i, a_i\in A, b_i\in B$$

的集合，这时因为

$$\sum a_ib_i-\sum a'_ib'_i=\sum a_ib_i+\sum(-a'_i)b'_i,$$

$$r\sum a_ib_i=\sum(ra_i)b_i, (\sum a_ib_i)r=\sum a_i(b_ir).$$

所以这个集成为 R 的理想，叫做 A，B 的积用 AB 表示，即

$$AB=\{\sum a_ib_i\,|\,a_i\in A, b_i\in B\}.$$

譬如，在整数环 Z 中，如果

$A=(12)$，$B=(21)$，那么 $(A,B)=(3)$，$AB=(252)$.

当 R 是交换环时，若 $A=(a)$，$B=(b)$，则 $(A,B)=\langle a,b\rangle$，$AB=(ab)$. 一般，假如 $A=\langle a_1,\cdots,a_m\rangle$，$B=\langle b_1,\cdots,b_n\rangle$，那么

$$(A,B)=\langle a_1,\cdots,a_m,b_1,\cdots,b_n\rangle,$$

$$AB=\langle a_1b_1,\cdots,a_1b_n,\cdots,a_mb_n\rangle.$$

这就是说，如果 A，B 是分别由 a_i，b_j，$i=1,\cdots,m$；$j=1,\cdots,n$，生成的理想，那么 (A,B) 是由 a_i，b_j 生成的理想，AB 是由 a_ib_j 生成的理想.

显然，$RA\subseteq A$，$AR\subseteq A$，如果 R 有单位元，那么 $A\subseteq RA$，$A\subseteq AR$，于是 $RA=AR=A$. 因此 R 是理想的乘法单位，这也就是 R 所以叫做单位理想的一原因.

同普通乘积的意义一样，R 的理想 A 的 n 乘幂 A^n 的意义是用下式来规定的：

$$A^1=A, A^{n+1}=AA^n, n \text{ 是正整数}.$$

为了方便，我们又常常把 A^0 写成 R 即 $A^0=R$. 当 $A^2=A$ 时，A 叫

做幂等理想，当 $A^n=0$ 时，A 叫做幂零理想. 这时 A 中任意 n 个元的乘积都是 0，即 $a_1\cdots a_n=0, a_i\in A$. 因此 A 中任意元都是幂零元. 任意元都是幂零元的理想，叫做幂零元理想. 所以幂零理想是幂零元理想，但反过来不一定成立.

我们容易知道，§3.1 定理 1 中交换环的幂零元子环是幂零元理想，但不一定是幂零理想.

由定义，我们容易知道

$$(AB)C=A(BC),$$

即对乘法，理想子环的结合律成立. 再因为 $A(B,C)$ 中任意元

$$\sum a_i(b_i+c_i)=\sum a_ib_i+\sum a_ic_i$$

在 (AB,AC) 中；反过来，(AB,AC) 中任意元

$$\sum a_ib_i+\sum a_jc_j=\sum a_i(b_i+0)+\sum a_j(0+c_j)$$

又在 $A(B,C)$ 中，所以 $A(B,C)=(AB,AC)$. 再

$$(A,B)(C,D)=(AC,AD,BC,BD).$$

假如 R 是交换环，那么

$$AB=BA,$$

这就是说，在交换环中，对乘法，理想的交换律成立. 但消去律不成立，即由 $AB=AC$，若 $A\neq 0$，未必有 $B=C$. 譬如，在由所有形如

$$a+3b\sqrt{-5}\,(a,b\text{ 是整数或零})$$

的数形成的环中，理想 A 等于 $(3,3\sqrt{-5})$，理想 B 等于 (3)，显然 A 不等于 B，但

$$A^2=(9,9\sqrt{-5},-45)=(3,3\sqrt{-5})(3)=AB.$$

我们知道，在整数环 Z 中，如果 $a\in(b)$，那么 $a\equiv 0(b)$，也就是 $a=rb$，即 a 能够被 b 整除. 现在我们根据这得到理想的整除.

假定 B 是 R 的理想，如果 $a\in B$，即 $a\equiv 0(B)$，我们就说 a 能够被理想 B 整除. 当理想 A 中任意元能够被 B 整除，即

$$A\subseteq B\text{，也就是 }A\equiv 0(B)$$

时，我们就说 A 能够用 B 整除，这时 B 叫做 A 的约理想、A 叫做

B 的倍理想.

要注意的是,在整数中,约数不能大于倍数,但在环中,约理想包含倍理想.假如我们把约理解为包含,倍理解为被包含,那么约理想与倍理想的关系就容易认清而不致混淆了.

环 R 中任意理想都包含零理想,因此零理想是任意理想的倍理想.单位理想 R 包含任意理想,因此 R 是任一理想的约理想,即 R 能整除任意理想.在整数中,$-1,1$ 能够整除任意整数,在这点上,R 与 $-1,1$ 非常类似,这是我们叫 R 做单位理想的另一原因.

显然,R 的理想 A,B 的和 (A,B) 是 A,B 的约理想,因此 (A,B) 是 A,B 的公约理想.但是 A,B 的任一公约理想都是 (A,B) 的约理想,所以 (A,B) 是 A,B 的**最大公约理想**.

假如环 R 有单位元,如果 $(A,B)=R$,那么我们叫 A、B 为**互质**.这时 A,B 除 R 外没有公约理想,并且 R 中任意元可以写成 A,B 中元的和.譬如,在整数环中,由两个互质数生成的两个理想是互质的.

同样,我们知道 $A\cap B$ 是 A,B 的公倍理想,并且 A,B 的公倍理想都是 $A\cap B$ 的倍理想,所以 $A\cap B$ 是 A,B 的**最小公倍理想**.

再因为 $AB\subseteq A$,$AB\subseteq B$,所以 $AB\subseteq A\cap B$,这就是说,A,B 的乘积 AB 是它们的最小公倍理想的倍理想.

我们容易知道,两个整数的最小公倍与最大公约的乘积等于这两个整数的乘积,因此在整数环 Z 中,理想 A,B 的最小公倍 $A\cap B$ 与它们的最大公约 (A,B) 的乘积等于它们的乘积 AB,即 $(A\cap B)(A,B)=AB$.但在一般交换环中,我们只能有

$$(A\cap B)(A,B)\subseteq AB,$$

这是因为

$$\begin{aligned}(A\cap B)(A,B)&=((A\cap B)A,(A\cap B)B)\\&\subseteq(BA,AB)=AB.\end{aligned}$$

当 A,B 是互质的理想,即 $(A,B)=R$ 时,那么 $AB=A\cap B$,也

就是说，这时 A,B 的乘积就是它们的最小公倍理想

下面，我们来介绍在一般交换环中理想的商的概念.

假定 A,B 是交换环 R 的理想，那么 R 中所有适合

$$rB\equiv 0(A)$$

的元 r 形成 R 的理想，叫做 A,B 的商[25]，用记号 $A:B$ 表示，即

$$(A:B)=\{r|r\in R,rB\subseteq A\},$$

这是因为，如果 r_1,r_2 适合上式，显然 r_1-r_2 以及 rr_1 也都适合上式，这里 r 是 R 中任意元. 特别

$$(0:B)=\{r|r\in R,rB=0\}$$

叫做 B 的**零化理想**.

由定义，我们容易知道

$$A:A=R,A:(0)=R,A\subseteq(A:B)\subseteq R,(A:B)B\subseteq A.$$

当 $B\subseteq A$ 时，$A:B=R$. 再

$$(A:B):C=(A:C):B=A:BC,$$

这是因为，由 $r\in(A:B):C$，我们就有 $rC\subseteq(A:B)$，即 $rCB=rBC\subseteq A$，所以 $r\in(A:BC)$，反过来也成立. 因此

$$(A:B):C=A:BC.$$

同样我们又有 $A:(B,C)=(A:B)\cap(A:C)$. 此外我们还有

$$(A_1\cap\cdots\cap A_n):B=(A_1:B)\cap\cdots\cap(A_n:B),$$

即

$$(\cap A_i):B=\cap(A_i:B),i=1,\cdots,n$$

这是因为由 $rB\subseteq\cap A_i$，就有 $rB\subseteq A_i$，反过来也成立.

在整数环 Z 中，(a)，$(b)\neq 0$ 的商 $(a):(b)$ 可以这样来求得，先把 a 分解因子，再删去其中能够整除 b 的因子，剩下的数如果是 c，那么 $(a):(b)=(c)$，譬如

$$(12):(3)=(4),(12):(21)=(4),(12):(5)=(12).$$

又因为这时 c 就是 a,b 的最大公约数 (a,b) 除 a 得到的商，所以我们又有 $(a):(b)=(a):(a,b)$. 这性质在一般交换环中也能够成立. 即

$$A : B = A : (A, B).$$

这是因为

$$A : (A, B) = (A : A) \cap (A : B) = R \cap (A : B) = A : B,$$

当 A, B 是互质理想时，我们有

$$A : B = A, B : A = B.$$

这是因为 $A \subseteq (A : B)$. 再假定 $r \in (A : B)$，那么 $rB \subseteq A$，但 $rA \subseteq A$，所以 $r(A, B) \subseteq A$，即 $rR \subseteq A$，因为 R 有单位元，所以 $r \in A$，因此 $(A : B) \subseteq A$. 于是 $A : B = A$. 同样，我们可以证明 $B : A = B$.

要注意的是，上面这性质的逆是不成立的. 譬如，在多项式环 $Z[x, y]$ 中，$(x) : (y) = (x)$，$(y) : (x) = (y)$，但 $((x), (y)) \neq (1)$.

假如 R 是非交换环，A、B 是 R 的理想，那么 R 中所有适合

$$rB \equiv 0(A) \quad (Br \equiv 0(A))$$

的元 r 形成 R 的理想，叫做 A, B 的右(左)商，用记号 $(A : B)_R$ $((A : B)_L)$ 表示. 同上面一样，我们容易得知

$$(A : A)_R = R, A \subseteq (A : B)_R,$$

$$(A : B)_R \cdot B \subseteq A, ((A : B)_R : C)_R = (A : CB)_R,$$

$$(A : (B, C))_R = (A : B)_R \cap (A : C)_R.$$

对于左商也有类似性质，读者试根据定义加以验证.

习　题　3.7

1. 求下列各商：

$$(6) : (3), (6) : (5), (3) : (9).$$

2. 假定 A, B, C 是环 R 的理想，$B \supseteq C$，试证.

$$C : A \subseteq B : A, A : B \subseteq A : C.$$

3. 试证下面三个关系等价，即假如有一个成立，那么其余两个也都成立：

(i) $A : B = A, A : C = A$，　(ii) $A : (B \cap C) = A$，　(iii) $A : BC = A$.

4. 假设 a, b 是整数，d 是 a, b 的最大公约，m 是 a, b 的最小公倍，即 $d = (a, b)$，$m = [a, b]$. $A = (a)$，$B = (b)$ 是整数环 Z 的理想，试证：

$$(A, B) = (d), A \cap B = (m).$$

5. 假如 B, C 都与 A 互质，那么 BC 及 $B \cap C$ 都与 A 互质.

6. 假定 $A_1, A_2, \cdots, A_n$ 是交换环 R 中两两互质的 n 个理想，试证

$$A_1A_2\cdots A_n = A_1\cap A_2\cap\cdots\cap A_n.$$

7. 试证一个理想与一个子环的和是子环，两个子环的和不是子环.

§3.8 极大理想、质理想

这节我们主要是介绍两个特殊的理想，它们在研究环时都占重要地位.

我们知道，环的任一理想至少有两个理想是它的包含集，一个就是它自身，一个是单位理想. 一般，除这两个理想外，可能还有包含它的理想.

定义 1 假定 N 是环 R 的理想，如果 $N\subset R$，并且 R 中不存在适合 $N\subset M\subset R$ 的理想 M，那么 N 叫做 R 的**极大理想**.

因此，极大理想除自身及单位理想是它的约理想外，不再有约理想，所以，我们又叫极大理想为**无因子理想**.

单位理想显然不是极大理想. 单环的零理想是极大理想. 在整数环 Z 中，由质数 p 生成的主理想 (p) 是极大理想. 这是因为，假如理想 $M\supset(p)$，那就有一整数 $a\in M$，但 $\overline{\in}(p)$，也就是说，M 中有不是 p 的倍数的数 a，因此 a，p 互质. 于是存在着两整数 r，s，使 $ra+sp=1$，但 $rp\in M$，$sp\in(p)$，因此 $1\in M$，所以 $M=Z$，这就是说 (p) 除了自身外，只有单位理想是它的约理想，所以 (p) 是极大理想.

由 §3.2 我们还知道 $\overline{Z}_p=Z-(p)$ 是域，也就是说，整数环 Z 关于极大理想 (p) 的同余环 $\overline{Z}$ 是域. 反过来，假如 $\overline{Z}_p$ 是域，那么 p 是质数，于是 (p) 是极大理想. 因此 (p) 是 Z 的极大理想的必要充分条件是 $\overline{Z}_p$ 是域. 一般在交换环中这性质也能成立，即

定理 1 有单位元的交换环 R 的理想 $N(\neq R)$ 是极大理想的必要充分条件是：同余环 $\overline{R}=R-N$ 成为域.

证明 假如 $\overline{R}$ 是域，那么 $\overline{R}$ 除零及自身外不再有理想，因此

N 是极大理想. 反过来,如果 N 是极大理想,那么 $\bar{R}$ 除零及自身外无其他理想,又因为 $\bar{R}$ 有单位元,于是由 §3.6 定理 2,$\bar{R}$ 是体,因此定理得证.

上定理虽然是理想 N 是极大的必要充分条件,但同时也是同余环 $R-N$ 成为域的必要充分条件. 要注意的是,这时 R 有单位元,假如 R 没有单位元,上定理的充分条件也能成立,但必要条件就不一定能够成立了. 譬如,在所有偶数形成的偶数环 S 中,(4)是极大理想,这是因为,假如$(4)\subset M$,$a\in M$,但$\bar{\in}(4)$,那么 $4,a$ 的最大公约数是 2,因此 $2=4r+sa$,这里 r,s 是整数. 于是 $2\in M$,所以 $M=S$. 这就是说,(4)除自身及 S 外,没有其他约理想,因此(4)是极大理想. 但 $2^2\equiv0(4)$,$2\not\equiv0(4)$,所以 $S-(4)$中有幂零元,因此它不成为体. 同样(6)也是 S 的极大理想但 $S-(6)$是域.

一般我们有

定理 2 环 R 的理想 N 是极大的必要充分条件是同余环 $\bar{R}=R-N$ 是单环.

证明 我们容易得知从 $R\sim R'$,那么 R 中理想在 R' 的象是 R' 的理想,R' 中理想在 R 的完全象源是 R 的理想,也就是说理想的象是理想,理想的完全象源也是理想,从 $R\sim\bar{R}$,如果 M 是 R 中包含 M 的真理想,即 $R\supset M\supset N$,那么 M 在 $\bar{R}$ 的象 $\bar{M}$ 是 $\bar{R}$ 中非零的真理想,反过来如果 $\bar{M}$ 是 $\bar{R}$ 中非零真理想,那么 $\bar{M}$ 在 R 的完全象源 M 是 R 中包含 N 的真理想,这样定理显然成立.

下面,再来介绍另一个重要理想.

我们知道,在整数环 Z 中,质数除自身及 1(包括正、负)外,不再有约数,在这点上,极大理想与质数类似. 再两个整数的积,如果能够用一个质数整除,那么这两个整数中至少有一个能够用这质数整除,这是质数的一个基本性质. 极大理想不一定都有这类似性质,但是环中有的理想确具有这性质.

定义 2 交换环 R 的理想 P,当 R 中两元 a,b 的积 ab 在 P 中时,a,b 中至少有一元在 P 中,也就是说当 $ab\equiv0(P)$时,

$$a \equiv 0(P) \text{或} b \equiv 0(P),$$

那么 P 叫做 R 的质理想.

单位理想 R 是质理想，因为对于 R 中任意元 a，这时都有 $a \equiv 0(R)$. 前面整数环 Z 的主理想 (p) 也是质理想. 这是因为，如果 $ab \equiv 0(p)$，那么 $ab = mp$，因此 a，b 中必有一数能够用 p 整除，即

$$a \equiv 0(p) \text{或} b \equiv 0(p).$$

假定交换环 R，R' 同态，即 $R \sim R'$，我们容易得知 R 的质理想在 R' 的象不一定是质理想，但 R' 的质理想在 R 的完全象源是 R 的质理想.

显然，交换环 R 的任意幂零元都包含在任一质理想中，因此，R 中所有质理想的交集包含 R 的所有幂零元，其逆亦成立. 即

定理 3 假定 R 是交换环，N 是 R 的所有质理想的交集，那么 N 是由 R 中所有幂零元组成的理想，也就是说 N 是 R 的最大幂零元环.

证明 假定 a 是 R 中元，但不是幂零元，如果我们能在 R 中求得一不包含 a 的质理想，那么 R 中任意非幂零元都不在 N 中，定理就成立.

显然，在 R 中有不包含 a 的任意幂的理想存在，因为零理想就是这样的理想. 由冲恩引理，我们有适合这条件的极大理想 P，如果 P 不是质理想，设 $x, y \in R$，$xy \in P$，而 $x, y \overline{\in} P$，因为 P 是极大，所以 $\langle P, x\rangle \supset P$，$\langle P, y\rangle \supset P$，因此有 $a^m \in \langle P, x\rangle$，$a^n \in \langle P, y\rangle$，于是 $a^{m+n} \in \langle P, x\rangle\langle P, y\rangle \subseteq P$，这与 P 不包含 a 的任意幂的假设矛盾，所以，P 是质理想，定理得证.

要注意的是上定理中的 N 不一定是质理想，即交换环中所有幂零元形成的理想子环不一定是质理想. 譬如 $\overline{Z}_8$ 中所有幂零元 $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ 形成质理想，但 $\overline{Z}_6$ 中只有零元是幂零元，这时零子环不是质理想. 因此质理想的交集不一定是质理想.

假如 R 是整环，那么零子环是质理想. 这是因为当 $ab = 0$ 时，a，b 中必有一为 0，即 $a = 0$ 或 $b = 0$. 反过来，假如交换环 R 的零子

环是质理想，那么 R 是整环，因此，零子环是质理想的必要充分条件是 R 为整环. 一般，我们有

定理 4 交换环 R 中的真理想 P 是质理想的必要充分条件是：同余环 $\overline{R}=R-P$ 是整环.

证明 假如 P 是质理想，因为 P 是理想，所以 $\overline{R}$ 成环，从 $\bar{a}\,\bar{b}=\bar{0}$，我们就得到 $ab\equiv 0(P)$；因此

$$a\equiv 0(P)\text{ 或 }b\equiv 0(P),$$

于是 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$，所以 $\overline{R}$ 是无零因子环，因此它是整环.

反过来，假如 $\overline{R}$ 是整环，由 $ab\equiv 0(P)$，我们就得到

$$\bar{a}\,\bar{b}=\bar{0},$$

于是 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$，因此 $a\equiv 0(P)$ 或 $b\equiv 0(P)$，所以 P 是质理想，于是定理得证.

要注意的是，在有单位元的交换环中，极大理想是质理想，但它的逆不成立，即质理想不一定都是极大的. 譬如，在整数环 Z 中，零理想是质理想，显然它不是极大理想. 又如在多项式环 $Z[x]$ 中，(x) 是质理想，但 $(x)\subset(2,x)\subset Z[x]$，因此它也不是极大理想. 再，在没有单位元的交换环中，极大理想不一定是质理想. 譬如，前面 S 中 (4) 就是 S 的极大理想，但不是质理想.

上面定义中 R 是交换环，关于一般环的质理想，1949 年麦珂另给出如下定义. 原因是在一般非交换环中如定义 2 中的质理想[26]为数不多.

定义 3 假如 P 是环 R 的理想，对 R 中任意两个理想 A,B，如果它们的积 $AB\equiv 0(P)$，我们就有 $A\equiv 0(P)$ 或 $B\equiv 0(P)$，那么 P 叫做 R 的质理想.

当 R 是交换环时，如果 P 是质理想，从 $ab\equiv 0(P)$，我们就有 $(a)(b)\equiv 0(P)$，所以 $(a)\equiv 0$ 或 $(b)\equiv 0$. 因此 $a\equiv 0(P)$ 或 $b\equiv 0(P)$，这就是说，定义 2 是这定义的特例.

显然，环 R 中任一质理想包含 R 中所有幂零理想. 假如 P 是 R 的质理想，那么 $\overline{R}=R-P$ 不含有非零的幂零理想.

假如把定义3中任意两个理想换成任意两个左理想，结果是一样的，这就是下面的定理.

定理5 环 R 的理想 P 是质理想的必要充分条件是对于 R 中任意两个左理想 L_1,L_2，如果 $L_1L_2\equiv 0(P)$，那么 $L_1\equiv 0(P)$ 或 $L_2\equiv 0(P)$.

证明 定理的充分性是显然的. 下面证明必要性.

因为 (L_1,L_1R)，(L_2,L_2R) 是 R 的理想，由 $L_1L_2\equiv 0(P)$，得

$$(L_1,L_1R)(L_2,L_2R)=(L_1L_2,L_1L_2R,L_1RL_2,L_1RL_2R)$$
$$\subseteq(L_1L_2,L_1L_2R,L_1L_2,L_1L_2R)\subseteq(P)$$

即 $$(L_1,L_1R)(L_2,L_2R)\equiv 0(P),$$

所以 $$(L_1,L_1R)\equiv 0(P)\text{或}(L_2,L_2R)\equiv 0(P)$$

因此 $$L_1\equiv 0(P)\text{或}L_2\equiv 0(P).$$

定理证毕.

上定理中的左理想假如都换成右理想，定理显然同样成立.

1956年生兹(A. D. Sands)证明了这样的定理：假定 P 是环 R 的质理想，那么 P_n 是全矩阵环 R_n 的质理想. 反过来，R_n 的质理想是 P_n，这里 P 是 R 的质理想. 再假如 N 是 R 的极大理想，如果 N 又是 R 的质理想，那么 N_n 是 R_n 的极大理想[26].

一个环，如果它的零子环是质理想，麦珂叫它做质环[27]. 因此，交换质环是整环，当然整环是质环. 质环不包含非零的幂零理想，质环中任意两个非零的理想的交集异于零. 再假定 R 是有单位元的环，全矩阵环 R_n 是质环的必要充分条件是 R 是质环[28].

假如 P 是环 R 的质理想，显然 $\overline{R}=R-P$ 是质环. 反过来也成立，即假如 $\overline{R}$ 是质环，那么 P 是质理想，这是因为如果 R 的理想 $A\not\equiv 0(P)$，$B\not\equiv 0(P)$，那么 $(A,P)\not\equiv 0(P)$，$(B,P)\not\equiv 0(P)$，因此 $\overline{R}$ 是质环，所以 $(A,P)(B,P)\subseteq(AB,P)\not\equiv 0(P)$，因此 $AB\not\equiv 0(P)$，即 P 是质理想. 再 R 是质环的必要充分条件是：左零化 R 的左理想的左理想是零理想或右零化 R 的右理想的右理想是零理想. 这些都是质环的基本性质[29]. 质环是一类重要的环，很多环的构造可

以由它来决定，只是目前质环本身的构造还不够清楚.

习 题 3.8

1. 假设 Q 为有理数域，那么 $Q[x]$ 中 (x) 是否为极大理想？

2. 试证 (x)，$(2,x)$ 都是 $Z[x]$ 的质理想.

3. 在高斯数环中，理想 (3)，$(1+i)$ 是否都是质理想？

4. 假设 P 是环 R 的理想，Q 是 R 中所有不在 P 中的元的集合，试证 P 是质理想的必要充分条件是 Q 对于乘法成半群.

5. 假定 A 是环 R 的理想，P 是环 A 的质理想，试证 P 是 R 理想.

6. 假设环 $R=R^2$，试证 R 的极大理想也是它的质理想.

7. 质环的中心是整环.

8. 环 R 的理想 P 是质理想的必要充分条件是对于 R 中任意元 a,b，如果 $aRb\subseteq P$，那么 $a\in P$ 或 $b\in P$.

9. 假定 N 是交换环 R 的理想，试证 $R-N$ 成域的必要充分条件是：

(1) N 是极大理想； (2) 如果 $x^2\equiv 0(N)$，那么 $x\equiv 0(N)$.

10. 试证有单位元的环有极大理想.

11. 假定 N 是环 R 的理想，如果 $N\neq 0$，并且 R 中不存在适合 $0\subset M\subset N$ 的理想 M，那么 N 叫做 R 的极小理想. 试证 N 是 R 的极小理想的必要充分条件是：N 是其中任意非零元生成的理想. 零理想虽然不能成为极小理想，但它有可能成为极大理想.

§3.9 主理想环中元素的因子分解

在整数环中，任意整数除因子的顺序外，可以唯一分解为质因子的乘积，也就是说，质因子分解是唯一的. 这是一个重要定理. 在任意环中这定理也能否成立？现在我们只在交换主理想环中来讨论这问题，这问题假如在主理想环中解决了，那么它也就基本上解决了.

定义 1 有单位元的整环，如果其中任意理想都是主理想，就叫做主理想环.

我们先给出下面一些重要的主理想环.

定理 1 整数环 Z 是主理想环.

证明 因为整数环 Z 是有单位元的整环,我们只要证明其中任一理想 N 是主理想就行了.

假如 $N=0$,显然它是主理想.假如 $N\neq 0$,那么它就含有一整数 $c\neq 0$,因此它也含有整数 $-c$,所以 N 含有正整数.现在假定 N 中所含的最小正整数是 a,如果我们能够证明 N 中任意数 b 都是 a 的倍数,即 $b=qa$,那么 $N=(a)$,因此 N 就是主理想了.

假定 b 用 a 除,我们就有

$$b=qa+r,0\leqslant r<a,$$

因为 $b\in N,a\in N$,所以

$$r=b-qa\in N.$$

但 a 是 N 中最小正整数,所以 $r=0$,因此 $b=qa$,于是定理得证.

多项式环 $Z[x]$ 虽然也是有单位元的整环,但由 § 3.6,我们得知它的理想不都是主理想,因此它不是主理想环.

定理 2 假定 F 是域,那么多项式环 $F[x]$ 是主理想环.

证明 首先,因为 F 的单位元 1 也是 $F[x]$ 的单位元,又因 F 是域,由 § 3.5 定理,$F[x]$ 是整环,因此 $K[x]$ 是有单位元的整环.

再,假定 $N\neq 0$ 是 $F[x]$ 的理想,$g(x)$ 是 N 中次数最低的一个多项式,$f(x)$ 是 N 中任一多项式,我们可以引用欧氏法式把 $f(x)$ 写成

$$f(x)=q(x)g(x)+r(x)$$

这里 $r(x)$ 是零元或者它的次数小于 $g(x)$ 的次数.同上面定理的证明一样,我们有 $r(x)=0$,所以 N 是主理想,因此定理得证.

下面,我们再给出一类重要的主理想环.

假定 R 是整环,如果对于其中任意非零的元 a,有整数 $\sigma(a)\geqslant 0$,并且对于 R 中任意元 $a\neq 0,b$,在 R 中有适合欧氏法式

$$b=qa+r,a\neq 0$$

的元 q,r,这里 $r=0$ 或 $\sigma(r)<\sigma(a)$,那么 R 叫做欧几里得环,或简

称为欧氏环.

显然,整数环 Z 是欧氏环,因为我们可以取 $\sigma(a)=|a|$. 多项式环 $F[x]$也是欧氏环,因为我们可以取 $\sigma(f(x))=f(x)$的次数.

定理 3 欧氏环是主理想环.

证明 假定$N\neq 0$是欧氏环R的理想,a是N中$\sigma(a)$最小的一元. 同定理1的证明一样,引用欧氏法式我们很容易知道N中任意元b是a的倍元,即$b=qa$,因此$N=(a)$,这就是说,R中任意理想都是主理想. 再我们命$R=(r)$,由上面的证明,我们得知R中任意元可以写成qr,因此r自身也是如此. 假如$r=er$,那么对于R中任意元$s=qr$,我们有$es=eqr=qer=s$,于是e是R的单位元. 这就是说,R是有单位元的整环,所以R是主理想环,因此定理得证.

要注意的是这定理的逆是不成立的,也就是说,主理想环不一定是欧氏环. 1949 年马士青(T. S. Matzkin)曾给了一个例来说明这问题,读者可参考原始资料[30].

现在,我们来讨论因子分解问题. 首先我们规定几个基本概念. 它们都与整数环中的类似.

假定R是有单位元e的整环,其中有的元有逆元,有的元没有逆元,可逆元是有逆元的元. 元a如果可以写成

$$a=r_1r_2\cdots r_n, r_i\in R,$$

就叫做a的**因子分解**,r_i叫做a的因子,也叫做a的**约元**,a又叫做r_i的**倍元**. 这时我们又说a可以用r_i整除. 显然,a可以写成

$$a=ae=(-a)(-e)=(-e)a(-e)$$

等等,更一般地,如果c是R中可逆元,它的逆元是c^{-1},我们又有

$$a=a\cdot cc^{-1}=ac^{-1}\cdot c=c^{-1}ac,$$

如这样含有可逆元做因子的因子分解,我们叫它做显然分解. 同在整数环中一样,这样的分解我们不讨论. 下面讨论的是r_i都不是可逆元的非显然分解.

假如a是b的约元,同时b又是a的约元,即$b=ma, a=nb$,

那么 $b=mnb$. 因为 R 是整环，所以 $mn=e$，这就是说 m,n 都是可逆元. 因此 a,b 相差只是一个可逆元的因子. 反过来，假如 $a=bc$，c 是可逆元，那么 $b=ac^{-1}$，因此 a 又是 b 的约元. 我们把相差只是一个可逆元因子的两个元叫做相伴. 于是 a,b 相伴的必要充分条件是 a,b 互为约元. 与 e 相伴的元是可逆元. 显然相伴关系是一个等价关系.

我们知道，任意与 a 相伴的元都是 a 的约元，任意可逆元也都是 a 的约元. 假如 b 是 a 的约元，而 b 是不可逆元，又不与 a 相伴，那么 b 就叫做 a 的**真约元**. 可逆元没有真约元.

同质数类似，我们有下面质元的概念.

定义 2 在有单位元的整环 R 中，元 $a\neq 0$，并且不是可逆元，如果它有真约元，就叫做**可分解元**；如果它没有真约元，就叫做**不可分解元**，或叫做**质元**.

于是，假如 p 是 R 的质元，由 $p=ab$，我们就得知 a,b 中有一是可逆元. 假如 q 是 R 的可分解元，那么在 R 中有非可逆元 a,b，使 $q=ab$. 又我们容易证明，质元与可逆元的乘积还是质元，也就是说，与质元相伴的元还是质元.

我们知道，在证明整数的因子分解时，要引用整数的大小顺序关系，但在主理想环中元没有顺序关系，下面的定理就是用来代替这关系的.

定理 4 假定 $a_1,a_2,\cdots,a_n,\cdots$ 是主理想环 R 中无穷多个元，并且任意 a_{i+1} 能够整除 a_i，那就有一个整数 m 存在，当 $i\geqslant m$ 时，所有的 a_i 都彼此相伴.

证明 假定 R 中各个 a_i 的所有倍元 ra_i，$r\in R$ 的集合是 N，b,c 是 N 中任意元，那么

$$b=ra_i,c=sa_j,i\geqslant j.$$

但 a_j 可以用 a_i 整除，也就是说 $a_j=ta_i$，因此

$$b-c=ra_i-sta_i=(r-st)a_i\in N,$$

所以 N 是 R 的理想. 假定 $N=(d)$，$d=ra_m$，那么任意 $a_i=kd=$

kra_m，即 a_m 是任意 a_i 的约元，但当 $i \geqslant m$ 时，a_i 又是 a_m 的约元，因此这时 a_i 与 a_m 相伴，这就是说，当 $i \geqslant m$ 时，所有的 a_i 都彼此相伴，因此定理成立.

对于有穷个元 $a_1, a_2, \cdots, a_m$，定理显然成立，因为这时 $N = (a_m)$.

现在，我们来讨论主理想环中元的分解.

我们容易知道，零元不能分解为有穷个质元的乘积；这是因为，假如

$$0 = r_1 r_2 \cdots r_n,$$

那么其中某个 $r_i = 0$，但零元不是质元. 同样，可逆元也不能分解为有穷个质元的乘积，因为如果

$$a = r_1 r_2 \cdots r_n,$$

那么
$$e = r_1 (a^{-1} r_2 \cdots r_n),$$

因此 r_1 是可逆元，但可逆元不是质元. 下面是分解定理.

定理 5 主理想环 R 中任意不是零元又不是可逆元的元，能够分解为有穷个质元的乘积.

证明 我们用反证法来证明. 假如定理不成立，a 是不满足定理的一元，也就是说，a 不能够分解为有穷个质元的乘积. 显然 a 不是质元，所以

$$a = bc,$$

这里 b, c 都不是可逆元，因此 b, c 都不与 a 相伴；并且 b, c 中最少有一元也不能够分解为有穷个质元的乘积. 设这元是 $b = a_1$. 再引用上面的方法就得到能够整除 a_1 但又不与 a_1 相伴的元 a_2，这样继续推求，我们就有

$$a, a_1, a_2, \cdots, a_n, \cdots,$$

这里 a_{i+1} 能够整除 a_i，但 a_{i+1} 与 a_i 不相伴，这与上面定理 4 矛盾，因此定理成立.

现在来讨论分解的唯一性.

在整数环中，证明因子分解的唯一性时要引用质数的一个基

本性质：两整数的乘积如果能够用一个质数整除，那么这两个整数中至少有一数能用这质数整除. 现在我们来证明在主理想环中，质元也有这基本性质. 我们知道，假如质元 p 有这性质，那么(p)就是质理想. 反过来，假如(p)是质理想，那么质元 p 就有这性质. 但是在主理想环中，极大理想是质理想，因此如果能够证明(p)是极大理想，那么 p 就有这性质了.

定理 6 在主理想环 R 中，质元 p 生成的理想(p)是极大理想.

证明 假定$(p)\subseteq(q)$，那就有 $p=rq$，因此 r,q 中必有一是可逆元. 如果 r 是可逆元，那么 $q=r^{-1}p$，所以$(q)=(p)$. 如果 q 是可逆元，那么 $qq^{-1}=e\in(q)$，所以$(q)=R$. 这就是说，(p)只有自身及单位理想是它的约理想，因此(p)是极大理想，所以定理得证.

于是，在主理想环中，两个元 a,b 的积 ab 如果能够用质元 p 整除，那么 a,b 中至少有一元能够用 p 整除.

再在主理想环中，可分解元 $q=ab$，这里 a,b 都不是可逆元，生成的理想(q)不是质理想，这是因为由 $ab\equiv0(q)$，如果 $a\equiv0(q)$，那么 $a=a'q$. 于是 $q=a'bq$，因此 $a'b=e$，这与 b 不是可逆元的假设不合.

于是，在主理想环中，质元生成的理想是质理想，可分解元生成的理想不是质理想，非零的质理想是极大理想.

最后，我们来证明质因子分解的唯一性. 所谓元 a 的因子分解是唯一的，就是说，如果 a 有两种因子分解

$$a=r_1r_2\cdots r_m=r'_1r'_2\cdots r'_n,$$

那么 $m=n$，并且每个 r_i 分别与某个 r'_i 相伴.

下面是主要定理

定理 7 主理想环 R 中任意不是零元又不是可逆元的元，除因子顺序及可逆元因子外，能够唯一分解为有穷个质元的乘积.

证明 假定元 $a\neq0$，又不是可逆元，由定理 5，a 可以分解为 m 个质元 p_i 的乘积，即 $a=p_1p_2\cdots p_m$. 如果它又可以分解为 n 个质

元 q 的乘积，即 $a=q_1q_2\cdots q_n$，那么

$$p_1p_2\cdots p_m=q_1q_2\cdots q_n.$$

现在，我们对于 m 用归纳法来证明这两种分解是一致的. 假如 $m=1$，因为这时 $a=p_1$ 是质元，但 q_i 都不是可逆元，于是 $n=1$，因此 $p_1=q_1$，所以这时定理成立. 假定对于 $m-1$ 定理成立，我们来证明对于 m 定理也能够成立. 因为 p_1 能够整除 a，也就是说能够整除 $q_1q_2\cdots q_n$，所以 p_1 必定能够整除某一个 q_i，我们适当改变 q_i 的顺序，使 p_1 能够整除 q_1，即

$$q_1=c_1p_1,$$

因为 q_1 是质元，所以 c_1 是可逆元，因此 p_1 与 q_1 相伴，于是我们有

$$p_1p_2\cdots p_m=c_1p_1q_2\cdots q_n=p_1(c_1q_2)\cdots q_n.$$

因为 R 是主理想环，所以也是整环，因此把 p_1 消去就得到

$$p_2\cdots p_m=(c_1q_2)\cdots q_n.$$

这时 p_i 的个数是 $m-1$. 根据归纳法假设，我们有 $m-1=n-1$，所以 $m=n$，并且 $p_2,\cdots,p_m$ 除顺序外分别与 $c_1q_2,\cdots,q_n$ 相伴，已知 p_1 与 q_1 相伴，所以定理成立.

于是，在主理想环中，元 a 如果能分解为有穷个质元的乘积，那么这有穷个质元的个数是一定的，这个数我们又叫做 a 的长.

在整数环中，可逆元只有 -1 及 1. 所以整数的质因子分解，除顺序外，相差只是一个符号. 又假如 F 是域，在多项式环 $F[x]$ 中，只有 F 中元是可逆元，所以这时多项式的质元分解，除顺序外，相差只是 F 中元的因子.

如所知在整数环 Z 中有因子分解定理；在多项式环 $Z[x]$ 中也有因子分解定理，但 $Z[x]$ 不是主理想环，而是关于主理想环 Z 的多项式环. 一般，在有单位元的整环 R 中，如果元素的因子分解定理能成立，可以证明在多项式环 $R[x]$ 中元素的因子分解定理也能成立. 因此，在主理想环或关于主理想环的多项式环中，元素的因子分解定理成立. 1955 年肯兹(G. Kantz)证明了它的逆定理：任一满足元素因子分解定理的环是主理想环或者是关于主理想环的

多项式环[31]. 这些,我们在这里都不详细论证了.

上面我们所说的环都是交换环. 关于非交换环,同样我们也有主理想环及欧氏环的概念,这只要把前面定义中的交换律除去就行了. 在非交换主理想环中,元素的因子分解定理也是成立的[32].

在交换环中,一个理想除因子的顺序外能否唯一地分解为质理想的乘积,这是所谓的理想分解问题,它是环论中主要问题之一. 由上面的定理7,我们容易得知,在主理想环中,任一异于零及自身的理想除因子的顺序外,能够唯一分解为质理想的乘积,因此理想分解的问题,在主理想环中是解决了的. 此外,在某些环中这问题也解决了[33]. 但在一般情况下,这问题到现在还没有得到解决.

习　题　3.9

1. 同余式 $6x\equiv 17(19)$ 是否有解? 为什么?

2. 试证在所有形如 $a+b\sqrt{-5}$,(a,b 是整数)的数组成的环中,

$$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$$

是两种不可约数的分解. 这就是说,在整环中,因子分解定理不一定成立.

3. 在主理想环中,所有与 a 互质(当 $(a,b)=(1)$ 时 a,b 叫做互质)的元所在的同余类(关于模 (a))对于乘法成群,怎样证明?

4. 试证体是欧氏环,高斯数环也是欧氏环.

5. 假定 R 是有单位元的整环,因子分解定理成立,那么质元生成的理想是质理想;非零的可分解元生成的理想不是质理想.

6. 假定 R 是满足因子分解定理并且有单位元1的整环.

$$f(x)=\sum_{i=0}^{n}a_ix^i$$

是 $R[x]$ 中元,d 是 $a_0,a_1,\cdots,a_n$ 的最大公约元,那么我们有 $f(x)=dg(x)$,当 $d=1$ 时,$f(x)$ 叫做**本原多项式**. 试证 R 中两个本原多项式的乘积仍然是本原多项式.

7. 假定 $f(x)$ 是 $R[x]$ 中多项式,如果 $f(x)$ 不能表为两个次数大于1的多项式的乘积,那么 $f(x)$ 叫做既约多项式,问 $R[x]$ 中既约多项式与质元有

无区别?

§3.10 多项式的零点

这节讨论多项式环$R[x]$中多项式$f(x)$零点的有关问题，它与$R[x]$中元素的因子分解有关. 这里R是有单位元的整环，所得到的结果与普通代数中的完全一致，因此也可以说是它的推广.

我们知道R的扩张环中一元a，如果满足多项式$f(x)\in R[x]$，也就是说$f(a)=0$，那么a就叫做$f(x)$的零点，或者叫做$f(x)$的根. 同普通代数中一样，我们有

定理1 a是多项式$f(x)$零点的必要充分条件是$f(x)$能够用$x-a$整除.

证明 假如$f(x)$能够用$x-a$整除，那么

$$f(x)=(x-a)g(x),$$

因此
$$f(a)=(a-a)g(a)=0,$$

所以a是$f(x)$的零点. 反过来，假如a是$f(x)$的零点，因为由欧氏法式，$f(x)$可以写成

$$f(x)=(x-a)q(x)+r,$$

于是
$$f(a)=(a-a)q(a)+r,$$

因此$r=0$，所以$f(x)=(x-a)q(x)$，即$f(x)$能够用$x-a$整除，于是定理得证.

一般我们有

定理2 环R中互异的m个元$a_1,\cdots,a_m$是多项式$f(x)$零点的必要充分条件是$f(x)$能够用$(x-a_1)\cdots(x-a_m)$整除.

证明 充分性易证，今只确证其必要性——命题$\pi(m)$(不赘述).

由定理1，$\pi(1)$为真. 若$\pi(k)$为真，则因设有环R中互异的$k+1$个元$a_1,\cdots,a_k,a_{k+1}$皆多项式$f(x)$的零点，从中任取k个，不妨设为$a_1,\cdots,a_k$，由归纳假设势必

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_k)g(x).$$

剩下的 α_{k+1} 适合 $(\alpha_{k+1}-\alpha_1)\cdots(\alpha_{k+1}-\alpha_1)g(\alpha_{k+1})=f(\alpha_{k+1})=0$. 注意到 $\alpha_{k+1}-\alpha_i(i=1,\cdots,k)$ 都不为零而 R 又是无零因子环，只好

$$g(\alpha_{k+1})=0.$$

因 $\pi(1)$ 为真，故 $g(x)=(x-\alpha_{k+1})q(x)$. 于是

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_k)(x-\alpha_{k+1})q(x)$$

—— $\pi(k+1)$ 亦真. 由归纳法知 $\pi(m)$ 为真($\forall\ m\in N$). 定理证毕.

于是，我们得到

定理3 假定 R 是有单位元的整环，$f(x)$ 是 $R[x]$ 中 n 次多项式，那么它在 R 中互异的零点不能多于 n 个.

要注意的是，这里 R 是整环，假如 R 不是整环，这定理是不能成立的[34]. 譬如 $\bar{Z}_6$ 是有单位元的交换环，但不是无零因子环，这时多项式 $f(x)=x^2-x$ 在其中有四个互异的零点 $\bar{0},\bar{1},\bar{3},\bar{4}$. 又如四元数体不是域，这时多项式 $f(x)=ex^2+e$ 在其中有六个互异的零点 $\pm i,\pm j,\pm k$.

根据上面的定理，我们有

定义 假定 $f(x)$ 能够用 $(x-\alpha)^k$ 整除，k 是大于1的整数，但不能用 $(x-\alpha)^{k+1}$ 整除，那么 α 就叫做 $f(x)$ 的 k **重零点**.

在讨论重零点时，需要导函数这个概念，但极限，连续等基本概念都不能在环中引用，所以我们不能用数学分析上的定义. 同普通代数中一样，若有 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$，则置

$$f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$$

称之为 $f(x)$ 的导函数. 由定义不难证明：

$$\{f(x)+g(x)\}'=f'(x)+g'(x),$$

$$\{f(x)\cdot g(x)\}'=f'(x)g(x)+f(x)g'(x),$$

$$\{f^m(x)\}'=mf^{m-1}(x)\cdot f'(x).$$

定理4 多项式 $f(x)$ 有重零点 α 的必要充分条件是 $f(x)$，$f'(x)$ 有公因式 $x-\alpha$.

证明 假如 α 是 $f(x)$ 的 $k(>1)$ 重零点，那么

$$f(x)=(x-a)^k g(x),g(a)\neq 0,$$

因此

$$f'(x)=(x-a)^k g'(x)+k(x-a)^{k-1}g(x)$$
$$=(x-a)^{k-1}\{(x-a)g'(x)+kg(x)\},$$

因为 $k-1>0$，所以 $(x-a)^{k-1}$ 是 $f(x)$，$f'(x)$ 的公因式，于是定理的必要性成立.

再假设 $x-a$ 是 $f(x)$、$f'(x)$ 的公因式，$f(x)=(x-a)g(x)$，因为 $f'(x)=(x-a)g'(x)+g(x)$，而 $x-a$ 又是 $f'(x)$ 的因式，所以 $x-a$ 也是 $g(x)$ 的因子，即 $g(x)=(x-a)h(x)$. 于是 $f(x)=(x-a)^2h(x)$，因此 a 是 $f(x)$ 的重零点，于是定理的充分性成立. 所以定理得证.

将来（§5.3）我们还会知道：当 R 是整环时，$R[x]$ 中任一多项式在 R 的适当扩张体中，至少有一零点存在，现在我们暂时承认这性质，于是由定理 4，即得

定理 5 多项式 $f(x)$ 有重零点的必要充分条件是 $f(x)$，$f'(x)$ 有次数大于零的公因式.

此外，我们还有下面的重要定理.

定理 6 任意复系数 $n(>0)$ 次多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,a_0\neq 0,$$

至少有一个复数根.

证明 假如我们能够证明多项式的系数都是实数时定理成立，那么系数是复数时定理也成立. 这是因为，命

$$\bar{f}(x)=\bar{a}_0x^n+\bar{a}_1x^{n-1}+\cdots+\bar{a}_{n-1}x+\bar{a}_n,$$

这里 $\bar{a}_i$ 是 a_i 的共轭复数，$f(x)$ 与 $\bar{f}(x)$ 的乘积

$$F(x)=f(x)\bar{f}(x)=b_0x^{2n}+b_1x^{2n-1}+\cdots+b_{2n},$$

由实际计算，我们容易得知

$$b_k=\sum_{i+j=k}a_i\bar{a}_j,k=0,1,\cdots,2n.$$

但 $\bar{b}_k=\sum\limits_{i+j=k}\bar{a}_ia_j=b_k$，因此，$F(x)$ 的系数都是实数，于是，根据

上面的假定，$F(x)$至少有一个复根 α，即 $F(\alpha)=f(\alpha)\overline{f}(\alpha)=0$. 如果 $f(\alpha)\neq 0$，那么$\overline{\overline{f}(\alpha)}=f(\overline{\alpha})=0$，这就是说，$\alpha$ 或者 $\overline{\alpha}$ 都是 $f(x)$的根，因此，我们只要就 $f(x)$的系数都是实数这种特殊情形来证明就行了.

假定 $n=2^l m$，m 是奇数，我们对于 l 用归纳法来证明.

当 $l=0$ 时，$f(x)$是奇数次多项式，这时如果 x 取适当大的正值，$f(x)$的符号与 a_0 的符号相同，如果 x 取绝对值适当大的负值，$f(x)$的符号与 a_0 的符号相反. 因为 $f(x)$是 x 的连续函数，由数学分析我们得知，$f(x)$有一个实根，这就是说当 $l=0$ 时，定理成立.

现在，我们假定多项式的次数能够用 2^{l-1}整除时定理成立，我们来讨论次数 $n=2^l m$ 的情况.

根据我们暂时承认的性质，容易知道 $f(x)$在复数体的适当扩张体中有 n 个根，假定这 n 个根是 $\alpha_1,\cdots,\alpha_n$，任取一实数 c，作

$$\beta_{ij}=\alpha_i\alpha_j+c(\alpha_i+\alpha_j),\ i<j,\ i,j=1,2,\cdots,n.$$

这时 β_{ij}的个数是

$$\frac{n(n-1)}{2}=\frac{1}{2}2^l m(2^l m-1)=2^{l-1}m',\ m'\text{ 是奇数.}$$

于是多项式
$$g(x)=\prod_{i<j}(x-\beta_{ij}),\ i,j=1,2,\cdots,n$$
的次数是 $2^{l-1}m'$，由中学代数我们容易得知，它的系数是 β_{ij}的初等对称多项式，当然也是 α_i 的对称多项式. 但 α_i 的初等对称多项式是 $f(x)$的系数，因此它们都是实数，所以 $g(x)$的系数也都是实数. 根据归纳法的假设，$g(x)$至少有一个复数根，即 β 中至少有一个是复数，也就是说，对于任一实数 c，我们至少有一个复数 β_{ij}，但实数的个数是无穷，而 i,j 只有$\frac{n(n-1)}{2}$对，因此在上面这些复数中，有 i,j 相同，而实数 c 不相同的复数

$$\alpha=\alpha_i\alpha_j+c_1(\alpha_i+\alpha_j),\ \beta=\alpha_i\alpha_j+c_2(\alpha_i+\alpha_j),$$

由于
$$\alpha_i+\alpha_j=\frac{\alpha-\beta}{c_1-c_2},\ \alpha_i\alpha_j=\frac{c_1\beta-c_2\alpha}{c_1-c_2}$$
都是复数，所以 α_i,α_j 是复系数多项式

$$x^2-(\alpha_j+\alpha_j)x+\alpha_i\alpha_j=0$$

的根. 显然 α_i,α_j 也都是复数，这就是说 $f(x)$ 至少有一个复数根，因此定理得证.

上定理就是我们普通所谓的**代数基本定理**. 远在 1629 年，吉拉尔(A. Girard，1595～1632)就有此猜想，1746 年达朗贝尔(J. E. R. D'Alembert，1717～1783)首先给了一个证明，但是不够严格，直到 1799 年高斯才圆满的解决了这问题. 此后高斯又给出了另外三个证明，上面的证明基本上就是他的第二个证明[35].

习 题 3.10

1. 假如 $R=Z-(5)$，试求 $R[x]$ 中多项式 x^5-1 在 R 中的零点.

2. 假定 m 是 n 的约数，试证 x^m-1 是 x^n-1 的因式.

3. 假定 R,R' 都是有单位元并且元数都是无穷的整环，R' 是 R 的扩张环，$f(x_1,\cdots,x_n)$ 是多项式环 $R'[x_1,\cdots,x_n]$ 中多项式，如果 $f(x_1,\cdots,x_n)\neq 0$，试证 R 中有元 $a_1,\cdots,a_n$ 使 $f(a_1,\cdots,a_n)\neq 0$.

参 考 文 献

[1] Passman, D. S. What is a group ring? Amer. Math. Monthly, 83 (1976), No. 3, 173～185.

[2] S. Warner, Rings with cyclic addition group, Amer. Math. Monthly, 71(1964), 449～450.

Ball, H. E. Rings with finitely many subrings, Math. Ann. 182(1969), 314～318.

Gilmer, Robert, A note on rings with only finitely many subrings, Scripta Math. 29(1973), 37～38.

[3] M. F. Smiley, Boolean rings, Amer. Math. Monthly, 54(1947), 114～115.

[4] R. Bear, Inverses and zero divisors, Bull. Amer. Math. Soc., 48 (1942), 630～638.

N. Jacobson, Some remarks on one-side inverses, Proc. Amer, Math.

Soc. ,1(1950),352～355.

M. Osima(大岛),Note on inverse in Rings,J. Gakugei Tokushima Univer. ,3(1953),21～23.

C. W. Bitzer,Inverses in rings with unity,Amer. Math. Monthly,70 (1963),315,

J. C. Shepherdson,Inverses and zerodivisors in matrix rings,Proc, London Math. Soc. ,1(1951),71～85.

[5] C. R. MacCluer, Order of smallest noncommutative ring, Amer. Math. Monthly,70(1963),441.

D. M. Bloom,Rings of order four,Amer. Math. Monthly,17(1964), 918～920.

K. E. Eldridge,Orders for finite noncommutative rings,Amer. Math. Monthly,75(1968),512～514.

[6] Y. Kenneth,Invertible elements in a finite ring,Amer. Math. Monthly,73(1966),95～96.

S. Z. Ditor,On the group of units of a ring,Amer. Math. Monthly,78 (1971),522～523.

[7] E. J. Taft,A finite ring R($\neq 0$) is a field if and only if it has no nozero nilpotent element and at most one nozero idempotent,Amer. Math. Monthly,75(1968),203.

T. P. Kezlan,Of a ring R with no nonzero divisors of zero and with every proper subring is finite,then R is a field of prime characteristic. Amer,Math. Monthly,74(1967),1016～1017.

[8] N. Ganesan,Properties of rings with a finite number of zero divisors I,Math. Ann. 157(1964),215～218;II,Math. Ann. 161(1965),241～246.

B. R. Mcdonald,Finite rings with unity(1974).

谭季伟、邱琦璋,元数等零因子个数平方的环,数学杂志,vol. 1 (1981),No. 2.

[9] Veselin Perit,Isomorphic rings,Amer. Math. Monthly,71(1964), 330.

[10] 华罗庚、万哲先，典型群(1963)，26.

[11] N. Jacobson, Structure of rings(1956), 186.

[12] Hua Loo-kang(华罗庚), On the automorphisms of a sfield, Proc. Nat. Acad. Sci. U. S. A., 35(1949), 386～389.

[13] 杨子胥，关于循环环及其幂等元，数学的实践与认识，3(1985)，73～76.

[14] A. Malcev, On the immersion of an algebraic ring into a field, Math. Ann., 113(1936), 686～691.

George Bergman, Integral domains embedded in primitive rings, Amer. Math. Monthly, 72(1965), 197～198.

A. J. Bowtell, On a question of Mal'cev, J. Algebra, 7(1967); 126～130.

[15] N. Jacobson, The theory of rings, (1943)31.

[16] O. Ore, Linear equations in non-commutative fields, Ann. of Math., 32(1931), 463～477.

A. A, Klein, Necessary condition for embeding rings into fields, Trans. Amer. Math. Soc. 137(1969), 141～151.

[17] N. H. McCoy, Remarks on divisors of zero, Amer. Math. Monthly, 49(1942), 286～295.

[18] W. R. Scott, Divisors of zero in polynomial rings, Amer. Math. Monthly, 61(1954), 336.

[19] Louis Weiner, Concerning a theorem of McCoy, Amer. Math. Monthly, 59(1952), 336.

[20] N. H. McCoy, Annihilators in polynomial rings, Amer. Math. Monthly, 64(1957), 28～29.

[21] R. D. Schafee, A remark on finite simple rings, Amer. Math. Monthly, 60(1953), 696～697.

[22] N. H. McCoy, The theory of rings(1967), 37～38.

[23] R. L. Kruse, Rings in which all subrings are ideals. I, Canad J. Math. 20(1968), 862～871.

[24] J. von Neumann, On reguler rings, Proc. Nat. Acad. Sci., 22(1986),

707～713.

[25] O. Steinfeld, On Ideal-quotients and prime ideals, Acta Math. Acad. Sci. Hung., 6(1953), 289～298.

[26] N. H. McCoy, Prime ideals in general rings, Amer. Jour. of Math., 71 (1949), 823～833.

[27] Sands, Arthur D., Prime ideals in Matrix rings, Proc. Glasgow Math. Assoc., 2(1956), 193～195.

[28] N. H. McCoy, The Theory of rings(1967), 72～73.

[29] N. J. Diviusky, Rings and radicals(1965), § 3.4.

R. E. Johnson, Prime rings, Duke Math. J., 18(1951), 799～809.

[30] T. S. Matzkin, The Eucliden algorithm, Bull. Amer. Math. soc., 55 (1949), 1142～1146.

H. H. Brungs, Left Euclidean rings, Pacific J. Math. 45(1973), 29～37.

[31] G. Kantz, Uber den Typus eines Zerlegungs Rings, Monatsh Math., 59(1955), 104～110.

—, Uber, Integrilats bereich mit eindeutiger Primelementzarlegung, Arch. Math., 6(1955), 397～402.

C. H. Giffen, Unique factorization for polynomials, Proc. Amer. Math. Soc., 14(1963), 366.

[32] N. Jacobson, The theory of rings(1943), 34.

[33] B. L. van der Waerden, Zur Produktzerlegung der Ideal in ganz-abgeschlessenen Ringen, Math. Ann., 101(1929), 298～308.

P. M. Cohn, Noncommutative unique factorization domain, Trans. Amer. Math. Soc., 109(1963), 313～331.

[34] R. A. Beaumont, Equivalent properties of a ring, Amer. Math. Monthly, 57(1950), 183.

[35] H. Zarsenhaus, On the fundamental theorem of algebra, Amer, Math, Monthly, 74(1967), 485～496.

C. Fefferman, An easy proof of the fundamental theorem of algebra, Amer. Math. Monthly. 74(1967), 854～855.

第4章

模与代数

这章介绍模与代数的最基本概念及一些基本性质．模与群、环类似的概念及性质，为了避免重复，一律从略．再因为它们在本书中引用不多，议论也不多，所以不作深入论述，只示大要而已．

§4.1 模

模是上世纪末克罗纳克尔提出来的．在本世纪40年代研究环的结构时，它占非常重要的地位，现在是代数中最重要的概念之一．模的前身可以说是向量空间，因此我们从向量空间开始．

在线代数中，我们已经知道向量空间的基本概念及性质，现在我们把这些概念来推广．

定义1 假定V是加群，它的元用$u,v,\cdots$表示，F是体(不一定是域)，它的元用$a,b,\cdots$表示，如果a,u的乘积au具备下列各性质，那么V叫做F的(左)向量空间，有时又简单地叫做F空间：

$1^\circ au\in V$， $2^\circ a(u+v)=au+av$，

$3^\circ (a+b)u=au+bu$， $4^\circ (ab)u=a(bu)$，

$5^\circ 1\cdot u=u$*，1是F的单位元，

---

* 因为$u=1\cdot u+(u-1\cdot u)$，命$1\cdot u=u'$，$u-1\cdot u=u_0$，那么$u=u'+u_0$，这时$1\cdot u'$为u'，对于F中任意元a，$au_0=0$．我们容易知道，所有的u'，u_0分别成为V的子空间V'，V_0，并且V是V'，V_0的直和(§5.4)，即$V=V'+V_0$．因为F中任意元零化V_0，所以在很多问题上讨论V时，可以把V_0略去，只讨论V'就可以．因此我们常常规定$1\cdot u=u$．

譬如复数域、四元数体都是实数域的向量空间．假如K是体F的扩张体，那么K是F的向量空间．又多项式环$F[x]$也是F的向量空间．

同有单位元的环一样，V的交换律可由其他条件推得．也就是说定义1中条件不是独立的．

由定义，我们有

$$(-a)u=a(-u)=-(au), 0a=a0=0.$$

再假如$au=0$，那么$a=0$或$u=0$，因此当$u\neq 0$时，如果$au=bu$，那么$a=b$.

假如V是F的向量空间，如果U是V的子群，又是F的向量空间，那么U叫做V的**子空间**．显然，一个零元形成一个子空间，叫做**零空间**．除自身及零空间外，不含其他子空间的空间叫做**既约空间**．

定义2 假定$u_1, u_2, \cdots, u_n$是F的向量空间V中元，如果F中有n个不完全是零的元$a_1, a_2, \cdots, a_n$存在，使

$$a_1u_1+a_2u_2+\cdots+a_nu_n=0,$$

那么$u_1, u_2, \cdots, u_n$叫做关于F**线性相关**；如果象这样的元$a_1, a_2, \cdots, a_n$不存在，也就是说上面那种关系只有$a_1, a_2, \cdots, a_n$都是零时才成立，那么$u_1, u_2, \cdots, u_n$就叫做关于F**线性无关**．

F向量空间中无穷多个元，如果其中某有穷个元关于F线性相关，那么它就叫做关于F**线性相关**；否则，也就是说，如果其中任意有穷个元关于F都是线性无关，那么它就叫做关于F**线性无关**．

于是，若干个元，如果线性相关，那么它们之间有线性关系，如果线性无关，那么它们之间没有任何线性关系．

以后引用上述定义时，如果不致引起混淆，为了简便，我们常常把其中"关于F"略去不写，只说线性相关、线性无关等．

我们很容易知道，V中一个元，只有零元线性相关，任意非零元线性无关．假如V的子集是线性相关，那么其中至少有一元，

譬如u_n,可以用其中其他有穷个元$u_1,u_2,\cdots,u_{n-1}$的一次式表示,即

$$u_n=a_1u_1+a_2u_2+\cdots+a_{n-1}u_{n-1};a_i\in F,$$

这时,我们又说u_n(关于F)是$u_1,u_2,\cdots,u_{n-1}$的**线性组合**,或者说u_n(关于F)与$u_1,u_2,\cdots,u_{n-1}$**线性相关**.反过来,假如n个元,其中有一元是其余元的线性组合,那么它们是线性相关.因此,若干个元线性相关的必要充分条件是:其中至少有一元是其余有穷个元的线性组合.

定义 3 假定V是F的向量空间,V中线性无关元的个数如果有最大数,这最大数,叫做V关于F的**维数**,用记号$(V:F)$表示.这时V又叫做关于F是$(V:F)$**维空间**,或者简称为是**有穷的**.如果V中线性无关元的个数没有最大数,那么V就叫做关于F是**无穷维空间**,或者简称为**无穷的**.假如K是体F的扩张体,那么K是F的向量空间,我们把K关于F的维数,又叫做K关于F的**次数**.

假定$(V:F)=n$,那么V中有n个元线性无关,并且任意多于n个的元都是线性相关.如果$u_1,u_2,\cdots,u_n$是V中线性无关的n个元,u是V中任意元,那么u是$u_1,u_2,\cdots,u_n$的线性组合,即

$$u=a_1u_1+a_2u_2+\cdots+a_nu_n,a_i\in F,$$

这表示显然又是唯一的.

定义 4 假定$u_1,u_2,\cdots,u_n,\cdots$是$F$空间$V$中元,如果$V$中任意元$u$可以用$u_1,u_2,\cdots,u_n,\cdots$中有穷个元的线性组合表示,那么$u_1,u_2,\cdots,u_n,\cdots$叫做$V$关于$F$的**生成元**,$V$关于$F$线性无关的生成元,叫做$V$关于$F$的**基底**.

假如$u_1,u_2,\cdots,u_n$是V关于F的基底,我们常常把V写成

$$V=Fu_1+Fu_2+\cdots+Fu_n.$$

这时V中任意元能够唯一地表为$u_1,u_2,\cdots,u_n$的线性组合。

于是,假如$(V:F)=n$,那么V中任意n个线性无关的元都形成关于F的基底,因此,有穷维空间都有基底.一般,引用冲恩

引理，我们容易证明任意空间都有基底[1].

我们知道一个向量空间的基底不是唯一的，但是各个基底的元数是一致的. 假如 V 有由 n 个元组成的关于 F 的基底，显然 $(V:F)\geqslant n$. 如果我们能够证明，这时 V 中任意 $n+1$ 个元线性相关，那么 $(V:F)=n$，因此基底的元数就是维数了. 这就是说，各个基底的元数是相等的，它们都等于维数. 要证明这个性质，需要下面定理.

定理1 假定 n 个未定元 $x_1,\cdots,x_n$ 的齐次线方程组

$$\sum_{j=1}^{n} a_{ij}x_j=0, i=1,2,\cdots,m,$$

中系数 a_{ij} 都是体 F 中元，并且 $n>m$，那么在 F 中，这方程组有非零解.

证明 我们对 m 用归纳法来证明.

当 $m=1$ 时，定理显然成立. 假定 $m-1$ 时定理成立，我们命

$$l_i=\sum_{j=1}^{n} a_{ij}x_j, i=1,2,\cdots,m.$$

如果所有的 $a_{i1}=0$，定理显然成立. 因此我们可以假设 $a_{11}\neq 0$. 于是线性方程组

$$l_1=0, l_2=0, \cdots, l_m=0$$

的任意解都是线方程组

$$l_1=0, l_2-a_{21}a_{11}^{-1}l_1=0, \cdots, l_m-a_{m1}a_{11}^{-1}l_1=0$$

的解，反过来也成立. 但线方程组

$$l_2-a_{21}a_{11}^{-1}l_1=0, \cdots, l_m-a_{m1}a_{11}^{-1}l_1=0$$

只有 $n-1$ 个未定元 $x_2,\cdots,x_n$，方程的个数是 $m-1$，由归纳法的假设，在 F 中，它有非零解 $x_i=\alpha_i, i=2,\cdots,n$. 于是

$$x_1=-a_{11}^{-1}(a_{12}\alpha_2+\cdots+a_{1n}\alpha_n), x_2=\alpha_2, \cdots, x_n=\alpha_n,$$

就是 $l_i=0, i=1,2,\cdots,m$，在 F 中的非零解，定理得证.

定理2 假设 n 个元 $u_1,u_2,\cdots,u_n$ 是 V 关于 F 的基底，那么 V 中任意 $n+1$ 个元关于 F 线性相关.

证明 假设 $v_1, v_2, \cdots, v_{n+1}$ 是 V 中任意 $n+1$ 个元，

$$v_i = a_{i1}u_1 + a_{i2}u_2 + \cdots + a_{in}u_n, i = 1, 2, \cdots, n+1.$$

我们的问题是在 F 中能否有不完全为零的 $n+1$ 个元 $b_1, b_2, \cdots, b_{n+1}$，使

$$b_1v_1 + b_2v_2 + \cdots + b_{n+1}v_{n+1} = 0.$$

我们把这式写成

$$\sum_{i=1}^{n+1} b_i v_i = \sum_{i=1}^{n+1} b_i \sum_{j=1}^{n} a_{ij}u_j = \sum_{j=1}^{n} (\sum_{i=1}^{n+1} b_i a_{ij}) u_j.$$

由定理1，齐次线方程组

$$\sum_{i=1}^{n+1} x_i a_{ij} = 0, j = 1, 2, \cdots, n,$$

在 F 中有非零解，假如我们挑选 $b_1, b_2, \cdots, b_{n+1}$ 就是这非零解，那么 $\sum_{i=1}^{n+1} bv_i = 0$，因此 $v_1, v_2, \cdots, v_{n+1}$ 线性相关，所以定理成立．

于是我们有

定理3 F 的向量空间 V 关于 F 的基底的元数等于它的维数 $(V:F)$.

譬如复数域是实数域的2维向量空间，$1, i$ 是它的基底．四元数体是实数域的4维空间，e, i, j, k 是它的基底．全矩阵环 F_n 是 F 的 n^2 维空间，$E_{ij}, i, j = 1, 2, \cdots, n$，是它的基底，这里 E_{ij} 是 F_n 中 i 行 j 列的元是1(F 的单位元)其它都是零的 n 阶矩阵，多项式环 $F[x]$ 是 F 的无穷维空间，$1, x, \cdots, x^n, \cdots$ 是它的基底．

下面是关于维数的一个重要关系．

定理4 假如 V 是体 K 的向量空间，F 是 K 的子体，如果 V 关于 F 是有穷维的，那么 V 关于 K 以及 K 关于 F 都是有穷维的．反过来，如果 V 关于 K 是有穷维的，K 关于 F 是有穷维的，那么 V 关于 F 也是有穷维的，再这三个维数间有关系

$$(V:F) = (V:K)(K:F).$$

证明 假如 V 关于 F 是有穷维，因为 $K \supseteq F$，所以 V 关于 K

也是有穷维．再假定 u 是 V 中非零元，显然所有形如 $au, a\in K$ 的元组成 V 的子空间 Ku，因为 V 关于 F 是有穷，所以 Ku 关于 F 也是有穷．命 $\alpha_1 u, \alpha_2 u, \cdots, \alpha_m u$ 是 Ku 关于 F 的基底，那么

$$au = a_1\alpha_1 u + a_2\alpha_2 u + \cdots + a_m\alpha_m u,$$

即

$$(a-(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m))u = 0,$$

于是

$$a = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m.$$

显然 $\alpha_1, \alpha_2, \cdots, \alpha_m$ 关于 F 线性无关，所以 $\alpha_1, \alpha_2, \cdots, \alpha_m$ 是 K 关于 F 的基底，这就是说，K 关于 F 是有穷的，因此定理的前段成立．下面我们来证明定理的后段．

假如 $(V:K)=n$，并且 $u_1, u_2, \cdots, u_n$ 是 V 关于 K 的基底；$(K:F)=m$ 而 $v_1, v_2, \cdots, v_m$ 是 K 关于 F 的基底，那么 mn 个元

$$v_i u_j, i=1,2,\cdots,m; j=1,2,\cdots,n,$$

是 V 中关于 F 线性无关的元．这是因为，如果

$$\sum_{j=1}^{n}\sum_{i=1}^{m} c_{ij} v_i u_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} c_{ij} v_i\right) u_j = 0, c_{ij}\in F,$$

因为 $u_1, u_2, \cdots, u_n$ 关于 K 线性无关，所以我们有

$$\sum_{i=1}^{m} c_{ij} v_i = 0, j=1,2,\cdots,n.$$

又因为 $v_1, v_2, \cdots, v_m$ 关于 F 是线性无关，所以

$$c_{ij}=0, i=1,2,\cdots,m; j=1,2,\cdots,n.$$

再假如 a 是 V 中任意元，因为 u_i 是 V 关于 K 的基底，所以

$$a = \sum_{j=1}^{n} a_j u_j, a_j\in K.$$

又因为 v_j 是 K 关于 F 的基底，所以

$$a_j = \sum_{i=1}^{m} b_{ij} v_i,$$

因此

$$a = \sum_{j=1}^{n}\sum_{i=1}^{m} b_{ij} v_i u_j.$$

这就是说，V 中任意元是 $v_i u_j$ 的线性组合，因此 $v_i u_j$ 是 V 关于 F 的基底，所以 $(V:F)=mn$. 于是定理的后段成立，因此定理成

立.

假如$(V:F)=1$,并且$V\supseteq F$,那么$V=F$. 这是因为,V中任意非零的元都是V关于F的基底,因此如果我们取F的单位元e做基底,那么$V=F\cdot e=F$. 于是由上面定理我们又得知,假如$V\supseteq K\supseteq F$,如果$(V:F)=(K:F)$,那么$(V:K)=1$,因此$V=K$. 如果$(V:F)=(V:K)$,那么$(K:F)=1$,因此$K=F$.

在定义1中,F中元a与V中元u的乘积我们是把a写在u的左边,所以这时我们又叫V做F的左向量空间. 假如我们把F中元写在V中元的右边,我们就叫V做F的右向量空间,这时,上面的结果都能够同样证明一一成立.

上面是介绍向量空间的基本概念和性质,大都是在线代数中所熟悉的. 下面我们来介绍模.

假如在向量空间定义1中,把体F换成环R或者说其中F不是体面是环R,把向量空间推广,我们就得到下面的重要概念:

定义5 假定M是加群,R是环,如果M中元m与R中元r的乘积rm仍在M中,并且还满足下列条件,那么M叫做(左)R-模

1. $r(m_1+m_2)=rm_1+rm_2$
2. $(r_1+r_2)m=r_1m+r_2m$
3. $(r_1r_2)m=r_1(r_2m)$.

F-向量空间V是F-模. 假如R是环,显然R的加群R^+可以看成左R-模,叫做R的左R-模,用${}_RR$表示. 同样我们也有R的右R-模R_R. 再任意交换群G可以看成是Z-模,这里Z是整数环. 如果把G写成加群这是显然的,如果写成乘群,命$na=a^n$,仍然有$n(ab)=(ab)^n=a^nb^n=na\cdot nb$. 这样把交换环的理论纳入模的理论,对环的某些理论的处理是比较方便的.

群有同态、同构,同样模也有同态、同构. 因为模的构造比群的要复杂些,与向量空间的基本一致. 所以模同态,同构比群的要求要多些. 下面的定义是与向量空间的线性变换一致的.

定义 6 假定 M、N 都是 R-模，σ 是 M、N 看成加群时的同态，如果

$$\sigma(rm)=r\sigma(m),r\in R,m\in M$$

也就是说当 $m\to n$ 时 $rm\to rn$，那么 σ 叫做模M 到模N 的同态．这时我们又说 M、N 同态．即 $M\sim N$．当 σ 又是双射时，叫 σ 同构；这时 M、N 同构，即 $M\simeq N$．

同群，环类似．假如 σ 是 R-模 M 到 R-模 N 的同态，那么 M 的象 $\sigma(M)$是 N 的子模，σ 的同态核 $\ker(M)$是 M 的子模．

上定义实际上是后面第六章的带算同态，带算同构．后面有较详的论述，这里就从略．下面作为一例．

假定 M，N 都是 R-模，M 到 N 的所有模同态集合用

$$\mathrm{Hom}_R(M,N)$$

表示，同§3.3 中一样 $\mathrm{Hom}_R(M,N)$是加群．显然其中不能有乘法，所以它不能成为环．但有可能成为模．因为

$$a\sigma(m)=a(\sigma(m)),a\in R,m\in M.$$

所以

$$a\sigma(m_1+m_2)=a\sigma(m_1)+a\sigma(m_2),$$

$$a\sigma(rm)=a(r\sigma(m))=ar\sigma(m).$$

当 R 是交换环时，我们有 $a\sigma(rm)=ra\sigma(m)$．因此 $a\sigma$ 是 M 的模同态，于是 $a\sigma\in\mathrm{Hom}_R(M,N)$．这就是说假如 M，N 都是 R-模，如果 R 是交换环，那么 $\mathrm{Hom}_R(M,N)$也是 R-模，

同向量空间的子空间一样，假如 N 是 R-模 M 的子加群，同时又是 R-模，那么 N 叫做 V 的子模．${}_RR$ 的子模是 R 的左理想，R_R 的子模是 R 的右理想．同群一样，模也有商模或差模．只由一个零元组成的 R-模叫做零模，用 0 表示．任意模 M 都有 0 及 M 自身这两个子模．只有这两个平凡子模的模，叫做单模．假如 R-模 M 是单模，如果 $RM\neq 0$，那么 M 叫做既约模，环 R 的左理想如果又是既约模，叫做 R 的既约左理想．环 R 有单位元时它的极小左理想是既约模，因此是 R 的既约左理想．再假如 M 是既约模，因

为 $RM\neq 0$,所以 $M=RM$. 又如果 $0\neq x\in M$,那么 $M=Rx$,这是因为如果 $Rx=0$,设 $N=\{nx\mid n=$整数或$0\}$,那么 $RN=0$. 于是 N 是 M 的子模,今 $N\neq 0$,所以 $N=M$,因此 $RM=0$. 这与 M 是既约的假设不合.

定理 5 假定 R 是环,那么 $_RR$ 是既约模的必要充分条件是 R 是体.

证明 假定 R 是体,显然 $R\cdot {_RR}=R^2\neq 0$,又因为体没有异于零及自身的左理想,所以 $_RR$ 除零及自身外没有其它子模,因此 $_RR$ 是既约模. 反过来,假定 $_RR$ 是既约 R-模,$0\neq a\in R$,所以 $Ra=R$,于是 $xa=b$ 在 R 中有解,所以 R 是体. 证毕.

假定 M 是 R-模,如果 $rM=0$,$r\in R$ 时 $r=0$,即 R 中任意非零的元不能零化 M,那么 M 叫做忠实模. 显然

$$A(M)=\{r\mid r\in R, rM=0\}$$

是 R 的理想,且 $A(M)\cdot M=0$. 若 $A(M)=0$,则 M 即忠实模.

假定 R-模 M 是既约模,如果 R 是单环,那么 M 是忠实模,这是因为 $A(M)$ 是 R 的理想,如果 $A(M)=R$,那么 $RM=0$,这与 M 是既约的假设不合,因此 $A(M)=0$.

定理 6 假定 M 是 R-模,那么 M 是 $\overline{R}=R-A_m(M)$ 模,并且是忠实模.

证明 因为 $A_m(M)\cdot M=0$,所以 $(r+A(M))M=rM$,因此 M 是 $\overline{R}$-模;若 $\overline{r}M=\overline{0}$,即 $(r+A(M))M=rM=0$,则 $r\in A(M)$,所以 $\overline{r}=\overline{0}$. 于是 M 是忠实 $\overline{R}$-模. 证毕.

假定环 R 有单位元 1,并且 $1\cdot m=m$,$m\in M$,那么 R-模 M 叫做酉模. 同循环群类似,由一个元素生成的模叫做循环模. 假如 R-模 M 是循环模,如果 R 有单位元,那么

$$M=Rx=\{rx\mid r\in R\}.$$

模的基底的概态与向量空间的一致. 即

定义 7 假定 M 是 R-模,$\{u_i\mid i\in I\}$ 是 M 的子集如果 M 中任意元 m 可以表为

$$m=\sum_{i=1}^{n} r_{m_i}u_{m_i}, r_{m_i}\in R$$

并且这表示又是唯一的，或者说$\{u_i\}$是线性无关的，那么$\{u_i\}$叫做M的基底．

任意R-模不一定有基底，譬如R是有单位元的环，x是它的右零因子，那么循环模Rx就没有基底．假如R-模M有基底，那么M叫做自由模．自由模也可同自由群同样定义：假定$X=\{x_i|i\in I\}$是非空集合，那么

$$\{\sum r_ix_i \mid r_i\in R, x_i\in X, r_ix_i\neq 0 \text{ 的只有有穷个}\}$$

形成的R-模，叫做自由模．显然这两个定义是一致的．

每个自由R-模能有不同基底，当R是有单位元的交换环时，有如向量空间，每个基底包含元素个数都一致．同§2.5定理6一样，任意R-模与某自由R-模的商模同构．其详见文献[2]．

习 题 4.1

1. 循环群(a)看成Z-模时是否是自由模？

§4.2 代 数

代数也可以说是来自向量空间或来自模．

假定域F的向量空间A是环，并且

(1) $$a(uv)=(au)v=u(av), a\in F, u,v\in A,$$

那么A叫做F的**代数**，或简单地叫做**代数**，F叫做它的**基础域**．因此A是满足条件(1)的酉F-模．代数是体时又叫做**可除代数**．假如A是F的n维向量空间，那么A叫做F的**n次代数**．

譬如，高斯数域是有理数域的2次可除代数，复数域是实数域的2次可除代数，四元数体是实数域的4次可除代数．假如G是n元群，那么群环$F[G]$是域F的n次代数，全矩阵环F_n是F的n^2次代数．假定环R的中心Z是体，那么R是Z或者是Z的子

域的代数，因此，任一体可以看成是它的中心的可除代数．

代数是一类特殊环．代数与环的主要差别在它们的加群，环的加群只是交换环，而代数的加群是域 F-模并且是酉模．

要注意的是，代数不一定包含它的基础域，也就是说，F 的代数 A 不一定包含 F．假如 A 有单位元 e，如果 $F\subseteq A$，因为

$$au=(au)e=u(ae)=ua$$

所以 F 在 A 的中心 $Z(A)$ 中，如果 $F\nsubseteq A$，显然 A 中所有形如 ae，$a\in F$ 的元组成的子域 Fe 与 F 同构，由§3.3的挖补定理，我们可以把 Fe 换成 F，因此 $F\subseteq A$．这就是说，有单位元的代数包含它的基础域，并且基础域在它的中心之中．

假定 A 是 F 的代数，如果 B 是 A 的子环，并且又是 F 的代数，那么 B 叫做 A 的子代数．代数 A 的子代数如果又是把 A 看成环时的理想，就叫做代数 A 的理想，要注意的是，代数 A 的理想与把 A 只看成环时的理想是有区别的，前者还要求它是子代数，当 A 有单位元时，两者是一致的．

代数 A 除零及自身外没有其它理想，并且 $A^2\neq 0$ 时，叫做单代数．因为 A^2 是 A 的理想，所以 $A^2=A$，这就是说 A 是单代数时 $A^2=A$．显然可除代数是单代数，但单代数不一定是可除代数．譬如全矩阵代数是单代数(§8.4)，但不是可除代数．

定理1 有穷次代数是可除代数的必要充分条件是它是无零因子环．

证明 定理的必要性是显然的．下面只证明充分性．

假定

$$A=Fu_1+\cdots+Fu_n,$$

$\alpha(\neq 0)$，β 是 A 中任意元，因为 A 是无零因子环，$u_1,\cdots,u_n$ 是基底，所以 $\alpha u_1,\cdots,\alpha u_n$ 也是基底，于是

$$\beta=\sum a_i(\alpha u_i)=\alpha\sum a_iu_i,$$

所以 $\alpha x=\beta$ 在 A 中有解，因此 A 是体．定理证毕．

假定

$$A=Fu_1+\cdots+Fu_n$$

是 F 的 n 次代数，由(1)，我们有

$$(au)(bv)=(ab)uv,$$

(2) $$(\sum_{i=1}^{n}a_iu_i)(\sum_{j=1}^{n}b_ju_j)=\sum_{i,j=1}^{n}a_ib_j(u_iu_j),$$

命

(3) $$u_iu_j=\sum_{r=1}^{n}c_{ij}^{(r)}u_r, c_{ij}^{(r)}\in F,$$

因为 $$u_i(u_ju_k)=\sum_{s=1}^{n}c_{jk}^{(s)}u_iu_s=\sum_{t=1}^{n}(\sum_{s=1}^{n}c_{jk}^{(s)}c_{is}^{(t)})u_t,$$

$$(u_iu_j)u_k=\sum_{t=1}^{n}(\sum_{s=1}^{n}c_{ij}^{(s)}c_{sk}^{(t)})u_t,$$

所以

(4) $$\sum_{s=1}^{n}c_{ij}^{(s)}c_{sk}^{(t)}=\sum_{s=1}^{n}c_{jk}^{(s)}c_{is}^{(t)}, i,j,k,t=1,\cdots,n.$$

反过来，假如向量空间 $A=Fu_1+\cdots+Fu_n$，其中任意两元 $\sum a_iu_i$，$\sum b_ju_j$ 的乘积是由(2)式来规定，并且(3)式中 $c_{ij}^{(r)}$ 又适合(4)式，我们容易证明 A 是 F 的代数.

于是代数 A 的构造由 F 中适合(4)式的 n^3 个元 $c_{ij}^{(r)}$ 唯一决定，所以 $c_{ij}^{(r)}$ 又叫做 A 的**构造元素**.

一个已知域的代数如何确定也就是说其构造如何，是代数的主要问题之一. 显然复数域的有穷次可除代数仍然是复数域，下面我们来讨论实数域的可除代数的构造.

我们知道实数域，复数域及四元数体分别是实数域的 1 次、2 次及 4 次可除代数. 但是实数域的可除代数是否只有这三类. 1877 年弗罗宾纽斯解答了这问题. 下面就是著名的弗罗宾纽斯定理.

定理 2 实数域的可除代数只有实数域，复数域及四元数体

三类.

证明 假设 F 是实数域,K 是 F 的 n 次可除代数,如果 $n=1$,那么 $K=F$,也就是说,这时 K 是实数域.

如果 $n>1$,那么 K 中有不是实数的数 α,这 α 当然是 F 的代数元. 因为 $F[x]$中既约多项式的次数是 1 或 2,而 α 不在 F 中,所以 $F[x]$中 α 适合的既约多项式的次数是 2. 我们假定这既约多项式是

$$x^2+px+q=0,p,q \text{ 都是实数},$$

因为它没有实根,所以 $q-\frac{p^2}{4}>0$,命

$$q-\frac{p^2}{4}=r^2,r \text{ 是实数},$$

那么 K 中元

$$i=\frac{1}{r}(\alpha+\frac{p}{2})$$

满足 $i^2=-1$,即 i 满足既约多项式 $x^2=-1$. 于是 $F(i)$是 F 的 2 次体. 如果 $n=2$,那么 $K=F(i)$,因为 $F(i)$显然与复数域同构,所以这时 K 是复数域.

如果 $n>2$,我们来证明 K 中包含有四元数体. 因为这时 K 中除 $F(i)$外还有元素,同上面一样,假定 j_0 是其中一元,那么 $j_0^2=-1$. 下面我们来计算 ij_0 及 j_0i. 因为 K 中任意元是 $F[x]$中 2 次多项式的零点,当然 $i+j_0,i-j_0$ 也是如此. 于是我们有

$$(1)\qquad \begin{cases}(i+j_0)^2=-2+ij_0+j_0i=a(i+j_0)+b,\\ (i-j_0)^2=-2-ij_0-j_0i=c(i-j_0)+d,\end{cases}$$

这里 a,b,c,d 都是实数,将上面两式相加,即得

$$-4=(a+c)i+(a-c)j_0+(b+d).$$

因为 j_0 不在 $F(i)$中,所以 $1,i,j_0$ 关于 F 线性无关,因此

$$a+c=0,a-c=0.$$

于是 $a=0,c=0$. 所以,由(1)中第一式即得

$$(2)\qquad ij_0+j_0i=2t,t=\frac{1}{2}(b+2).$$

再根据(2)式,我们来求四元数体中的 j. 命 $j'=j_0+ti$,则有

$$ij'+j'i=i(j_0+ti)+(j_0+ti)i=ij_0+j_0i-2t=0,$$

但

$$j'^2=-1+t(ij_0+j_0i)-t^2=-1+t^2$$

必须是一个负数，即 $j'^2<0$，因为不如此，j' 是实数，那么 $1,i,j_0$ 就线性相关，这与假设不合．命 $j'^2=-s^2$，s 是实数，我们就有

$$j=\frac{1}{s}j',$$

这时，$j^2=-1$，并且 $ij+ji=\frac{1}{s}(ij'+j'i)=0$，即

$$ij=-ji.$$

设 $k=ij$，得 $ij=-ji=k$，再由计算容易得知

$$k^2=-1, ki=-ik=j, jk=-kj=i.$$

又 $1,i,j,k$ 线性无关，这是因为，如果

$$k=a+bi+cj, a,b,c \text{ 是实数},$$

用 i 左乘，即得

$$\begin{aligned}-j&=ai-b+ck=ai-b+c(a+bi+cj)\\&=ca-b+(a+bc)i+c^2j.\end{aligned}$$

因为 $1,i,j$ 线性无关，所以 $c^2=-1$，这与 c 是实数的假设不合．因此，K 含有由所有四元数 $a+bi+cj+dk$，$a,b,c,d\in F$，组成的四元数体做它的子体，如果 $n=4$，那么 K 就是四元数体．

最后，我们来证明 $n\leqslant 4$．假如 $n>4$，那么 K 中又有元 $l^2=-1$，并且它与 $1,i,j,k$ 线性无关．同(2)式一样，我们有

$$il+li=a, jl+lj=b, kl+lk=c, a,b,c \text{ 是实数},$$

于是

$$\begin{aligned}lk&=(li)j=aj-ilj=aj-i(b-jl)=aj-bi+ijl\\&=aj-bi+kl=aj-bi+c-lk,\end{aligned}$$

因此 $aj-bi+c=2lk$．用 k 右乘，即得

$$ai+bj+ck=-2l.$$

这与 i,j,k,l 线性无关的假设不合，所以 n 不能大于 4．

于是定理完全得证．

此外,1932 年亚尔伯脱(A. A. Albert, 1905～)及哈缨(H. Hasse, 1898～)曾证明[3],关于代数体的可除代数是正规可除代数*. 再1933年曾炯之(1896～1940)曾证明,函数体 $\Omega(x)$ 的可除代数只有 $\Omega(x)$ 自身[4]. 这些都是重要的构造定理.

在代数中,假如把它的乘法结合律这个条件挖去,那么它就叫做**非结合代数**. 因此,非结合代数虽然对乘法也是闭合的,但不再是环了. 与这相应,上面我们介绍的代数,因为它满足乘法结合律,所以,我们又常常叫它做**结合代数**.

假定 A 是非结合代数,对于 A 中任意元 a,b,c,如果

$$ab=ba,(a^2b)a=a^2(ba),$$

那么,A 叫做**约当**(P. Jordan, 1902～　　)**代数**;如果

$$ab=-ba,a(bc)+b(ca)+c(ab)=0,$$

那么 A 叫做**李**(M. S. Lie, 1842～1899)**代数**. 如果

$$a^2b=a(ab),ba^2=(ba)a$$

那么 A 叫做**交错代数**,显然结合代数是交错. 反过来不一定成立. 这些都是在非结合代数中,目前性质知道得比较多的代数[5].

习　题　4.2

1. 试证 $E_{ij}(i,j=1,2,\cdots,n)$ 是全矩阵代数 F_n 关于 F 的底.

2. 试证 F 的代数的中心仍然是 F 的代数.

3. 试用§3.4 习题3 证明:任意没有单位元的代数能够嵌入于有单位元的代数.

4. 假如单环 R 关于它的中心是有穷维,试证 R 中任意正则元都是可逆元.

5. 试证1次代数 Fu 是结合代数.

6. 假定 A 是结合代数,其中任意两元 a,b 的乘积 ab 如果用 $a\circ b=ab+$

---

* 假如 A 是域 F 有单位元的代数,如果 F 是 A 的中心,那么 A 叫做 F 的**正规代数**. 正规代数是可除代数时,叫做**正规可除代数**. 因此四元数体是实数域的正规可除代数.

ba 代替，那么 A 是约当代数，如果 A 对乘法不是交换，ab 用 $a\times b=ab-ba$ 代替，那么 A 就是李代数．

参 考 文 献

[1] N. 贾柯勃逊著，抽象代数（黄缘芳译），科学出版社，卷2，第九章，215～216.

[2] 冯克勤，交换代数基础，高等教育出版社(1986)，§2.1，§2.2.

[3] A. A. Albert and H. Hasse, A determination of all normal division algebras over an algebraic number field, Trans. of Amer. Soc., 34 (1932), 722～726.

[4] Tsen C. C. (曾炯之) Division algebren über Funktionenkörper, Gott. Nach. (1933), 335～339.

——, Algebren über Fuunktionenkörper, Gottingen dissertation (1934).

[5] Report of a conference on linear algebras, Ram's Head Inn., Jane (1956), 6～8.

R. D. Schafer, An introduction to nonassociative algebras (1966).

第5章

域论

体的基本概念在前面已简单介绍，这章将详细讨论交换体即域的构造．因为任一体可以看成为它的子体的扩张体，它可以由子体添加若干元扩张而成，所以我们讨论体的构造从扩张入手，先讨论代数扩张体，再讨论超越扩张体；我们的重点在代数扩张体而且以有穷的为主．

关于域的构造，斯太尼兹(E. Steinitz，1871～1928)于1910年在Crelle杂志上发表长达142页的论文，全面地系统地详加论述．1930年这长篇论文另发行单行本，是域论的经典著作[1]．1952年斯那泼尔(E. Snapper，1913～)曾把斯太尼兹这套理论应用到完全准质环*上，建立了完全准质环的构造，读者如有余力，可参考文献[2]．

要注意的是这里讲的只是域的结构，一般体虽然是域的自然推广，但它的性质除某些特殊情况的外，一般的都非常复杂[3]．再体在一般代数中所起的作用远不及域在交换代数中那样重要，目前的议论也不多，在本书中当然从略．

---

* 一个交换环如果有单位元，并且它的根基是极大理想，它就叫做完全准质环．也就是说，假如交换环 R 有单位元，D 是它的根基，如果 $R-D$ 成体，那么 R 就是完全准质环．显然，体是完全准质环．

§5.1 添　　加

我们知道，假定 K 是一般体，K 的子集 F 对于 K 的两种结合法如果形成为体，就叫做 K 的子体．这时 K 又叫 F 的扩张体．K 可以看成为自身的子体．由§2.2，我们又知道，K 的子集 F 成为子体的必要充分条件是：

1°F 含有非零的元；

2°假如 $a,b\in F$，那么 $a-b\in F$，并且当 $b\neq 0$ 时，$ab^{-1}\in F$．

假如 K 是体 F 的扩张体，L 是 K 的子体，并且又是 F 的扩张体，即 $K\supseteq L\supseteq F$，那么 L 叫做 K,F 的中间体．假如 M 是 K 的子集，显然在 K,F 的中间体中存在着包含 M 的中间体，因为 K 自身就是这样的一个中间体．在 K,F 的中间体中，所有包含 M 的交集又是包含 M 的中间体，因此它就是 K 中包含 F 及 M 的最小子体．这体我们用 $F(M)$ 来表示，叫做 F 添加 M 扩张的体．当 $M=\{u_1,\cdots,u_n\}$ 时，我们又用记号 $F(u_1,\cdots,u_n)$ 表示．在§3.5中，环的添加是用方括弧表示，这里体的添加我们用圆括弧．显然，

$$F\subseteq F(M)\subseteq K,F(K)=K,$$

当 $M\subseteq F$ 时，

$$F(M)=F.$$

我们知道 $F(M)$ 包含 F 及 M 的元，因此包含 F 中元与 M 中元的一切有理结合（加，减，乘，除）．但所有这些有理结合的元自身显然形成为一个体，因为它包含 F 及 M，所以它就是 $F(M)$．这就是说，$F(M)$ 是由 F 中元与 M 中元的一切有理结合的元形成的体．当 K 是域时，$F(M)$ 中元就是系数是 F 中元的 M 中元的有理函数，因此 $F(M)$ 也是域．

因为在 F 中元与 M 中元的任一有理结合中，M 中元只出现有穷个，所以 $F(M)$ 中任意元包含在 M 的某有穷子集 N 的添加 $F(N)$ 中，因此 $F(M)$ 是若干个有穷集添加的并集．这也就是说，任

意集的添加可以由有穷集添加的并集而成.

再假如 M_1, M_2 是 K 的子集,显然

$$F(M_1)(M_2)=F(M_2)(M_1).$$

又

$$F(M_1\cup M_2)=F(M_1)(M_2),$$

这是因为,$F(M_1\cup M_2)$包含 F 及 M_1, M_2,于是也包含 $F(M_1)$及 M_2,因此包含 $F(M_1)(M_2)$,所以 $F(M_1\cup M_2)\supseteq F(M_1)(M_2)$. 反过来,$F(M_1)(M_2)$包含 $F(M_1)$及 M_2,于是它也包含F 及 $M_1\cup M_2$,因此 $F(M_1)(M_2)\supseteq F(M_1\cup M_2)$. 所以 $F(M_1\cup M_2)=F(M_1)(M_2)$.

于是我们得知,

$$F(\alpha_1,\cdots,\alpha_n)=F(\alpha_1)\cdots(\alpha_n).$$

即有穷集的添加可以由有穷多回陆续添加一个元而成,因此一个元的添加如果研究清楚了,那么任意集的添加也可以说基本上清楚了. 所以一个元的添加是最基本的,我们叫它做单扩张. 假如 K 是 F 的单扩张体,$K=F(\alpha)$,这 α 又叫 K 关于 F 的本原元.

§5.2 质域、特征数

因为我们讨论体的构造是由子体的添加入手,所以我们首先来讨论体的最小子体,即所谓质体的构造.

同讨论群、环、模时一样,体 K 的所有子体(包含自身)的交集仍然是子体. 这子体显然除自身外不再包含其他子体. 象这样只有自身做子体的体,叫做质体. 因此,任意体都含有质体做子体.

再假如 K 有两个互异的质子体 F_1, F_2,因为 $F_1\cap F_2$ 也成为体,所以 F_1, F_2 就有异于自身的子体,这与 F_1, F_2 是质体的假设不合,因此,在 K 的子体中是质体的只有唯一个,于是我们得到

定理 1 任意体包含一个而且只一个质体.

单位元群是只有自身做子群的群,由零元组成的环是只有自身做子环的环,任意群包含单位元群,任意环也包含零元组成的

环．在这点上，质体与单位元群、零元组成的环类似．

我们容易得知，有理数体 Q 是质体，整数环 Z 关于质数 p 的同余环 $\bar{Z}_p=Z-(p)$ 也是质体．下面，我们来证明它的逆，即质体只有这两种类型．

假如 F 是质体，e 是它的单位元，那么

(1) $$\cdots,-2e,-e,0,e,2e,\cdots$$

都是 F 中元，它们形成整环 R，结合法是：

$$me+ne=(m+n)e, me\cdot ne=mne.$$

同§2.2中讨论循环群的构造一样，下面分两种情形来讨论：

1．假如(1)中元互不相等，也就是说当 $ne=0$ 时，$n=0$，那么 R 与整数环 Z 同构，但 Z 的分式域是有理数域 Q，因此 R 的分式域也就与有理数域 Q 同构，这就是说，F 含有与 Q 同构的子域，所以这时 $F\simeq Q$.

2．假如(1)中元有相等的，也就是说，有非零的整数 n 适合 $ne=0$. 假如 p 是适合 $ne=0$ 的最小正整数，那么 p 是质数，这是因为，如果 $p=mn$，那么

$$pe=mne=me\cdot ne=0,$$

因此 $me=0$ 或 $ne=0$，这与 p 是最小的性质不合．同§2.2中一样，(1)中任意元与

$$0,e,\cdots,(p-1)e$$

中某一元相等，由§3.2，我们得知这 p 个元形成一个域，它与 $\bar{Z}_p$ 同构．这就是说 F 有与 $\bar{Z}_p$ 同构的子域，所以这时 $F\simeq\bar{Z}_p$

一个体，它的单位元 e 的任意倍如果都异于零，如第1种情形，我们叫这体的**特征数是零**．如果 e 的某质数 p 倍是零，如第2种情形，我们就叫这体的**特征数是 p**. 假如我们把体看成加群，如果它的单位元 e 的阶是无穷，那么它的特征数就是零；如果 e 的阶是有穷，并且是某质数 p，那么它的特征数就是 p.

譬如有理数域、实数域、复数域及四元数体的特征数都是零，而 $\bar{Z}_p$ 的特征数是 p.

引用特征数这个概念，由上面的讨论，我们得到

定理 2 质体的特征数如果是零，它与有理数域 Q 同构，如果是 p，它与整数环 Z 关于 (p) 的同余环 $Z-(p)$ 同构.

假定 F 是体 K 的子体，因为 F 的单位元就是 K 的单位元，所以 F 的特征数与 K 的特征数一致. 这就是说，体与它的子体的特征数是相等的，或者说它们的质体是一致的.

显然质体是域，因此质体也叫做质域. 再一个体的质域包含在它的中心之中.

特征数这概念是体的一个重要概念，它对于体的构造有决定性的作用. 下面我们再来讨论它的基本性质.

假定 a 是体 K 中任意非零的元，n 是整数，K 的特征数如果是零，那么由 $na=0$，我们就有 $na\cdot a^{-1}=ne=0$. 所以 $n=0$. 因此这时 $na=0$ 的必要充分条件是 $n=0$. K 的特征数如果是 p，那么 $pa=pe\cdot a=0$. 假如 $na=0$，同 §2.2 中一样，由 $n=qp+r$，$na=qpa+ra=0$，我们就有 $r=0$，所以 $n\equiv 0(p)$. 因此这时 $na=0$ 的必要充分条件是 $n\equiv 0(p)$. 一般，当 K 的特征数是零时，$ma=na$ 的必要充分条件是 $m=n$. 当 K 的特征数是 p 时，$ma=na$ 的必要充分条件是 $m\equiv n(p)$.

于是，体 K 的特征数如果是零，那么 K 中任意非零元的任意倍都异于零，如果是 p，那么 K 中任意元的 p 倍都是零. 因此特征数根据定义虽然是单位元的性质，但它也是体中任意元的公共性质.

普通代数中讨论的数是实数或复数，它们都是在特征数为零的体中. 在特征数是 p 的体中，有些运算规则就与普通不同，下面的公式就是普通代数中所不允许的.

定理 3 假设域 K 的特征数是 p，而 a,b 是其中任意两元，那么

$$(a+b)^p=a^p+b^p,\ (a-b)^p=a^p-b^p.$$

证明 因为 K 是域，我们有

$$(a+b)^p=a^p+C_1^pa^{p-1}b+\cdots+C_{p-1}^pab^{p-1}+b^p,$$

式中

$$C_i^p=\frac{p(p-1)\cdots(p-i+1)}{i!},1\leqslant i\leqslant p-1.$$

因为C_i^p是整数，其中p又不能消去，所以C_i^p能够用p整除，即$C_i^p\equiv0(p)$，于是

$$(a+b)^p=a^p+b^p.$$

再因为 $$a^p=(a-b+b)^p=(a-b)^p+b^p,$$

所以 $$(a-b)^p=a^p-b^p,$$

定理证毕.

1963年卡斯拉(S. Càslar)证明了上定理的逆，即假如体K的特征数是p，如果对于K中任意元a,b，我们有$(a+b)^p=a^p+b^p$，那么K是域[4]. 因此特征数是p的体是域的必要充分条件是：对于其中任意元a,b，有$(a+b)^p=a^p+b^p$.

因为体的特征数又是把体看成加群时其中任意非零元的阶数，环也可看作为加群，所以我们可以把特征数这个概念推广到环上面来. 这样得出下面的概念.

环R看成加群时，各元的阶数中如果没有最大数，我们就说R的特征数是零；如果最大数是正数m，我们就说R的特征数是m. 因此，假如R有单位元e，当e的阶是无穷时，显然这时R的特征数是0；当e的阶数是m时，因为对于R中任意元a，

$$ma=m(ea)=(me)a=0\cdot a=0,$$

也就是说，任意元的阶数不大于m，所以这时R的特征数是m. 于是，有单位元环的特征数概念也可以同体一样来定义[5].

假如R是无零因子环，a,b是其中非零的两元，那么由$ma=0$，我们就有$mb=0$，这是因为

$$(mb)a=b(ma)=0,$$

而$a\neq0$，所以$mb=0$. 这就是说，在无零因子环中，所有非零元的阶数是一致的. 因此，无零因子环的特征数就是其中所有非零元

的公共阶数．再我们又容易得知，无零因子环的特征数同体的特征数一样，或是零，或者是质数．

要注意的是，体的特征数 p 有性质 $pa=0$，由§2.2习题5，显然环的特征数 m 也有性质 $ma=0$. 再体的特征数与它的子体的特征数相同，对环就不一定．譬如在§3.4习题3中，(R,Z) 的特征数是0，假如 R 的特征数是 p，那么 (R,Z) 的特征数与子环 R 的就不同．

习 题 5.2

1. 假定 F 是体 K 的质域，试证 F 是 K 的中心的子体．
2. 试求 $Z[i]-(1+i)$ 的特征数．这里 $Z[i]$ 是高斯数环．
3. 假设域 K 的特征数是 p，试证

$$(a_1+a_2+\cdots+a_m)^{p^n}=a_1^{p^n}+a_2^{p^n}+\cdots+a_m^{p^n}, a_i\in K,$$

$$(a-b)^{p-1}=\sum_{i=0}^{p-1}a^ib^{p-1-i}.$$

4. 假定在特征数是 p 的体 K 中，任意元满足多项式 $x^p-x=0$，试证

$$K\simeq Z-(p).$$

5. 试证布尔环是交换环，并证明它的特征数是2.
6. 假定 K 是体，p 是质数，$|K|\geqslant p$，如果对于 K 中任意元 a,b 总有 $(a+b)^p=a^p+b^p$，那么 p 是 K 的特征数．

§5.3 单扩张域

因为任意域可以从质域的添加而成，而质域的构造已经清楚，因此现在就需要讨论单扩张域了．

前面两节的讨论是对一般体而言，这节讨论的体都是域．下面，我们来讨论域 F 的单扩张域 $F(\alpha)$ 的构造．

假设 F 是域，α 是一个元，因为要求 $F(\alpha)$ 是域，所以 α 与 F 中任意元能够交换，于是 $F(\alpha)$ 包含由所有 α 的多项式 $\sum a_i\alpha^i$，$a_i\in F$，组成的环 R，这环因为在体中，所以是整环．因此，如果 R 成

体，那么 R 就是所求的 $F(\alpha)$，如果 R 不成体，那么 R 的分式域就是 $F(\alpha)$.

我们把 R 与多项式环 $F[x]$ 来比较．显然对应

$$\sum a_i x^i \to \sum a_i \alpha^i$$

是 $F[x]$ 到 R 上的同态．由§3.6定理6，我们有

$$R \simeq F[x]-N,$$

这里 N 是同态核，它是由 $F[x]$ 中所有以 α 为零点的多项式组成的理想．假如 $F[x]$ 中除零元外，没有以 α 为零点的多项式，那么 $N=0$；假如 $f(x)$ 是 $F[x]$ 中以 α 为零点次数最低的多项式，因为 $F[x]$ 是主理想环，所以 $N=(f(x))$.

1. 当 $N=0$ 时，

$$R \simeq F[x],$$

因此 R 的分式域就是 $F(\alpha)$. 但 R 的分式域与 $F[x]$ 的分式域同构，而 $F[x]$ 的分式域是由未定元 x，系数是 F 中元的所有有理函数形成的有理函数域 $F(x)$，所以这时单扩张域 $F(\alpha)$ 与有理函数域 $F(x)$ 同构．

2. 当 $N=(f(x))$ 时，因为 R 是整环，所以 $f(x)$ 是既约多项式，于是由§3.9定理6，$(f(x))$ 是极大理想，再由§3.8定理1，$F[x]-(f(x))$ 是域，因此 R 也是域，所以这时 $R=F[\alpha]$ 就是单扩张域 $F(\alpha)$.

当 $N=0$ 时，α 是 F 的超越元，因此 $F(\alpha)$ 叫做 F 的**超越单扩张域**．§3.5中多项式环 $R[x]$ 也可说是环 R 的超越单扩张环．当 $N=(f(x))$ 时，α 是 F 的代数元，因此 $F(\alpha)$ 叫做 F 的**代数单扩张域**．这时 $F[x]$ 中 α 适合的最低次数多项式 $f(x)$ 的次数又叫做 α 关于 F 的**次数**．根据欧氏法式，我们不难得知，$f(x)$ 除相伴的外是唯一的．再我们还可以假定 $f(x)$ 的次数大于1，因为如果 $f(x)=ax+b$，那么 $\alpha=-\frac{b}{a}\in F$，因此 $F(\alpha)=F$．引用这定义，由上面的讨论，我们有

定理1 假定 F 是域，α 是元，如果 α 是 F 的超越元，那么 F 的超越单扩张域 $F(\alpha)$ 与未定元 x 的有理函数域 $F(x)$ 同构：

$$F(\alpha)\simeq F(x).$$

如果 α 是 F 的代数元，并且 α 是 $F[x]$ 中既约多项式 $f(x)$ 的零点，那么 F 的代数单扩张域 $F(\alpha)$ 与 $F[x]-(f(x))$ 同构：

$$F(\alpha)\simeq F[x]-(f(x)).$$

于是，超越单扩张域 $F(\alpha)$ 中任意元是 α 的有理函数，它的运算法则与把 α 看成未定元 x 时的有理函数运算法则一样．代数单扩张域 $F(\alpha)$ 就是多项式环 $F[\alpha]$，假如 α 适合的既约多项式 $f(x)=\sum_{i=0}^{n}a_ix^i$，因为 $\alpha^n=-a_n^{-1}(a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1})$，所以 $F(\alpha)$ 中任意元可以表为 $\sum_{i=0}^{n-1}c_i\alpha^i$，$c_i\in F$ 的形状，并且这种表示又是唯一的，这是因为，如果

$$\sum_{i=0}^{n-1}a_i\alpha^i=\sum_{i=0}^{n-1}b_i\alpha^i,$$

那么

$$\sum_{i=0}^{n-1}(a_i-b_i)\alpha^i=0,$$

但 α 的次数是 n，所以 α 不能适合 $F[x]$ 中次数小于 n 的多项式，因此 $a_i=b_i$，$i=0,\cdots,n-1$．这就是说，$F(\alpha)$ 是由次数小于 n 的 α 的所有多项式形成的体，它的运算法则与把 α 看成为未定元 x 时的多项式的运算法则一样，只是当运算的结果是次数不小于 n 的 α 的多项式时，我们要引用 $f(\alpha)=0$ 把它化为 $\sum_{i=0}^{n-1}c_i\alpha^i$ 的形状，或者说，把 α 看成为 x 时，$F(\alpha)$ 中元的运算法则与 $F[x]$ 中多项式的一样，只是我们要对 $f(x)$ 取同余式就是了．

譬如 Q 是有理数域，$\alpha=\sqrt{2}$，那么 $Q(\sqrt{2})$ 中任意元可以唯一地表为 $a+b\sqrt{2}$，这里 a,b 是有理数．例如，

$$\frac{3+5\sqrt{2}}{4+\sqrt{2}}=\frac{(2+5\sqrt{2})(4-\sqrt{2})}{4^2-2}=\frac{1}{7}+\frac{17}{14}\sqrt{2}.$$

单扩张域 $K=F(\alpha)$，当 α 是超越元时，它关于 F 的次数是无穷；当 α 是 n 次代数元时，因为 $1,\alpha,\cdots,\alpha^{n-1}$ 是 K 关于 F 的基底，所以它的次数是 n，即 $(K:F)=n$.

一般添加 $\alpha_1,\cdots,\alpha_n$ 于域 F 扩张的域 $F(\alpha_1,\cdots,\alpha_n)$ 也可以同样求得．因为添加 $\alpha_1,\cdots,\alpha_n$ 于 F 扩张的域就是每回添加一元陆续添加 $\alpha_1,\cdots,\alpha_n$ 于 F 扩张的域．因为我们考虑的是域，当 $\alpha_1,\cdots,\alpha_n$ 都是 F 的超越元时，$F(\alpha_1,\cdots,\alpha_n)$ 中任意元是系数是 F 中元的 $\alpha_1,\cdots,\alpha_n$ 的有理函数；当 $\alpha_1,\cdots,\alpha_n$ 都是 F 的代数元时，$F(\alpha_1,\cdots,\alpha_n)$ 中任意元是系数是 F 中元的 $\alpha_1,\cdots,\alpha_n$ 的多项式．

现在，我们来讨论两个单扩张域之间的关系，为了更好地说明，我们引进一个新概念．

定义 假如 K,K' 都是体 F 的扩张体，σ 是 K 到 K' 上的同构，如果

$$\sigma(a)=a,a\in F,$$

也就是说，σ 不使 F 中任意元变动，那么 σ 叫做 K,K' 关于 F 的**同值映射**，这时 K,K' 又叫做关于 F **同值**．

譬如 $a+b_i\to a-b_i$，a,b 是实数，就是复数域关于实数域的自同值．

假如 $F(\alpha),F(\beta)$ 是 F 的超越单扩张域，因为 $F(\alpha),F(\beta)$ 与 $F(x)$ 不只都是同构，而且关于 F 又都是同值，因此 $F(\alpha),F(\beta)$ 关于 F 同值，它们的同值映射是

$$\frac{f(\alpha)}{g(\alpha)}\to\frac{f(\beta)}{g(\beta)},$$

它不使 F 中任意元变动并且把 α 变为 β.

假如 $F(\alpha),F(\beta)$ 是 F 的代数单扩张域，并且 α,β 是 $F[x]$ 中同一个 n 次既约多项式 $f(x)$ 的零点．因为这时 $F(\alpha)$ 与 $F(\beta)$ 中任意元可以分别写成 $\sum_{i=0}^{n-1}a_i\alpha^i$，$\sum_{i=0}^{n-1}a_i\beta^i$，我们容易知道

$$\sum_{i=0}^{n-1}a_i\alpha^i\to\sum_{i=0}^{n-1}a_i\beta^i$$

就是它们的同构映射，这映射不使 F 中任意元变动，并且把 α 变为 β，因此 $F(\alpha)$ 与 $F(\beta)$ 关于 F 同值．

由上面的讨论，我们得

定理 2　假设 $F(\alpha)$，$F(\beta)$ 是域 F 的单扩张域，如果 α,β 都是 F 的超越元，那么 $F(\alpha)$，$F(\beta)$ 关于 F 同值；如果它们都是 F 的代数元，并且又都是 $F[x]$ 中同一既约多项式的零点，那么 $F(\alpha)$，$F(\beta)$ 关于 F 同值．上面这两种同值都有不使 F 中任意元变动而把 α 变为 β 的同值映射．

这也是说，把 $F[x]$ 中 $f(x)$ 的两个零点 α,β 添加于 F 得到的两个单扩张 $F(\alpha)$，$F(\beta)$ 是一致（同构）的．

我们知道，代数单扩张域的本原元不是唯一的，所以代数单扩张 $F(\alpha)$、$F(\beta)$ 关于 F 同值时，α,β 不一定就是 $F[x]$ 中同一既约多项式的零点．因此它们的同值映射不一定就把 α 变为 β．譬如 Q 是有理数域，因为 $Q(\sqrt{2})=Q(2\sqrt{2})$，当然 $Q(\sqrt{2})$，$Q(2\sqrt{2})$ 关于 Q 同值，但 $\sqrt{2}$，$2\sqrt{2}$ 不是 $Q[x]$ 中同一既约多项式的零点，因此它们没有把 $\sqrt{2}$ 变为 $2\sqrt{2}$ 的自同值映射．但是如果 α 在 $F(\beta)$ 的象是 α'，那么 $F(\alpha)\simeq F(\alpha')$．于是 $(F(\alpha'):F)=(F(\beta):F)$，因为 $F(\alpha')\subseteq F(\beta)$，所以 $F(\alpha')=F(\beta)$，这就是说，$F(\beta)$ 有这样的本原元 α'，它是 $F[x]$ 中 α 适合的既约多项式的零点．

在 §2.4 中，我们介绍了群的共轭元及共轭子群的概念，在体中我们也有与这类似的概念．

假定 K 是 F 的扩张体，K_1，K_2 是 K，F 的中间体，如果它们关于 F 同值，那么 K_1，K_2 就叫做关于 F 共轭，有时 K_1，K_2 也叫做关于 F 的**共轭体**，这时 K_1 中元 α_1 在 K_2 中的象 α_2，叫做 α_1 关于 F 的**共轭元**，而 α_1，α_2 又叫做关于 F 共轭．因此 F 中元与自身共轭．再从定理 2，我们容易得知域 F 的任意两个超越元是 F 的共轭元；F 的代数元成为共轭的必要充分条件是它们为 $F[x]$ 中同一既约多项式的零点．

上面介绍代数单扩张域 $F(\alpha)$ 的构造时，是已给出 α，其实 $F(\alpha)$ 只与 α 适合的既约多项式 $f(x)$ 有关，α 不过是一个记号而已．因此，只要已知 $f(x)$，并不需要求出 α，我们同样可以求得 $F(\alpha)$．这样，我们又得到包含 $f(x)$ 零点的 F 扩张域．

我们从 $F[x]-(f(x))$ 来做出所求的 $F(\alpha)$．我们知道，$F[x]-(f(x))$ 中元是 $F[x]$ 中 $(f(x))$ 的同余类．当 $a,b\in F$ 时，如果 $a\neq b$，显然 $a\not\equiv b(f(x))$，因此 $\bar{a}\neq\bar{b}$，所以 $F[x]-(f(x))$ 中所有 F 中元所在的同余类组成与 F 同构的子体．引用 § 3.3 的挖补定理，我们就得到包含 F 并且与 $F[x]-(f(x))$ 同构的域 K．再因为 $f(x)$ 的次数大于 1，所以在体 K 中，x 所在的同余类 $\bar{x}$ 不是 F 中元，我们用 α 来代替同余类 $\bar{x}$．这样，K 就是由系数是 F 中元的 α 的多项式组成的体，它包含 α 及 F 并且与 $F[x]-(f(x))$ 同构．我们假定 $f(x)=\sum a_i x^i$，那么在 $F[x]-(f(x))$ 中，

$$\overline{f(x)}=\overline{\sum a_i x^i}=\sum \bar{a}_i\,\bar{x}^i=\bar{0},$$

当 a_i 代替 $\bar{a}_i$，α 代替 $\bar{x}$ 时，我们就有 $\sum a_i\alpha^i=0$，这就是说，在 K 中 $f(\alpha)=0$，即 α 就是 $f(x)$ 的零点，所以 K 就是代数单扩张域 $F(\alpha)$．于是我们有

定理 3 假定 F 是域，$f(x)$ 是 $F[x]$ 中既约多项式，那就存在与 $F[x]-(f(x))$ 同构的 F 代数单扩张域 $F(\alpha)$，其中 α 是 $f(x)$ 的一个零点．

要注意的是，定理中所谓的零点 α 只是一个记号，它只是代表 $F(x)-(f(x))$ 中 x 所在的同余类 $\bar{x}$ 而已．

由上定理我们得知，$F[x]$ 中任意既约多项式 $f(x)$ 在 F 的扩张域 $F[x]-(f(x))$ 中有零点 α，这与 § 3.10 中代数基本定理类似．一般就是下面是关于多项式零点的**克罗纳克尔**(L. Kronecker 1823～1891)**定理**．

定理 4 假如 $f(x)$ 是多项式环 $F[x]$ 中多项式，那么在域 F 的扩张域中，存在着包含 $f(x)$ 的零点的域．

证明 假设 $g(x)$ 是 $f(x)$ 在 $F[x]$ 中的既约因式，那么把 $g(x)$ 的零点 α 添加于 F 得到的与 $F[x]-(g(x))$ 同构的单扩张域 $F(\alpha)$ 就是所求的域，因此定理成立.

假如 $F[x]$ 中任意多项式的零点都在 F 中，那么 F 叫做代数闭域，因此，如果 F 是代数闭域，那么 $F[x]$ 中任意既约多项式的次数都是 1，于是添加 F 的任意代数元于 F 得到的扩张域仍然是 F 自身，也就是说，这时 F 不能够再用代数扩张来扩大. 譬如复数域就是代数闭域，这是因为根据代数基本定理，任意系数是复数的多项式的零点仍是复数，因此复数域不能再用代数扩张来扩大.

引用冲恩引理，我们不难证明任意域可以代数扩张成为代数闭域，并且域 F 的代数闭域关于 F 同值[6].

代数基本定理是以复数域为基础，定理 4 是以抽象的代数域为基础，由于抽象系统的出现，代数基本定理渐失去原有地位，复数域也被代数闭域所代替.

习 题 5.3

1. 假如 α 是 $Q[x]$ 中既约多项式 $g(x)=x^2-5x+7$ 的零点，试把

$$\frac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}$$

写成 α 的多项式，这里 Q 是有理数域.

2. 试求 $Q(\sqrt[3]{2})$ 中元 $1+\sqrt[3]{2}+\sqrt[3]{4}$ 的逆元.

3. 假定 Q 是有理数域，试证 $Q(i)\simeq Q[x]-(x^2+1)$.

4. 假如 F 是实数域，α 是既约多项式 $g(x)=x^2+x+1$ 的零点，求作代数单扩张域 $F(\alpha)$，并且在 $F(\alpha)$ 中分解 $g(x)$ 为既约因式的乘积.

5. 假如 F 是特征数为 p 的质域，x 是未定元，$K=F(x)$，试求将既约多项式 y^p-x 的一零点 $\alpha=x^{\frac{1}{p}}$ 添加于 K 得的扩张域 $K(\alpha)$，并且在 $K(\alpha)$ 中分解 y^p-x.

6. 假如 $f(x)$，$p(x)$ 是 $F[x]$ 中的多项式，并且 $p(x)$ 是既约的，如果在 F 的扩张域 K 中，$f(x)$，$p(x)$ 有公共零点，试证 $f(x)$ 能够用 $p(x)$ 整除.

7. 假如多项式环$F[\alpha]$是域，那么$F[\alpha]$是F的代数单扩张域.

§5.4 代数扩张体

前面介绍了扩张体的基本概念及基本性质，并且讨论了单扩张域的构造．此后各节是讨论一般扩张体的构造，主要是代数扩张域的构造．

假如K是域F的扩张体，$(K:F)=n$，α是K中任意元，那么$n+1$个元

$$1,\alpha,\cdots,\alpha^n$$

线性相关，因此

$$c_0+c_1\alpha+\cdots+c_n\alpha^n=0,$$

所以α是多项式

$$f(x)=c_0+c_1x+\cdots+c_nx^n$$

的零点．这就是说，K中任意元都是F的代数元．如这样的F扩张体，其中任意元都是F的代数元时，叫做F的代数扩张体或F的代数体．F的扩张体如果不是代数扩张体，就叫做F的超越扩张体，或F的超越体．代数体如果是域，叫做代数域，超越体如果是域，叫做超越域．

譬如，复数域是实数域的代数域，实数域是有理数域的超越域，F的超越单扩张域是F的超越域．

根据上面的讨论，我们有

定理1 体F的有穷次扩张体是F的代数体．

于是，域F的代数单扩张域$F(\alpha)$是F的代数域．一般，假如$\alpha_1,\cdots,\alpha_n$都是F的代数元，因为F的代数元也是F的扩张体的代数元，由§4.1定理4，我们不难得知域$F(\alpha_1,\cdots,\alpha_n)$是$F$的有穷次域，因此它是$F$的代数域，这就是说，由代数元扩张的域是代数域．所以，在F的扩张域中，F的代数元的和、差、积、商仍然是F的代数元．

假如域 K 对于它的子域 F 的次数是有穷，那么在 K 中存在着有穷个元 $\alpha_1,\cdots,\alpha_n$，使得 $K=F(\alpha_1,\cdots,\alpha_n)$.

要注意的是，定理 1 的逆不成立，即 F 的代数域不一定是 F 的有穷次域．譬如，所有代数数形成的域是有理数域 Q 的代数域，显然它不是 Q 的有穷次域．

假定 L 是体 K、F 的中间体，即 $K\supseteq L\supseteq F$，如果 K 是 F 的代数体，显然 K 是 L 的代数体，L 是 F 的代数体．下面就是它的逆．

定理 2　假定 K 是 L 的代数域，L 是 F 的代数域，那么 K 是 F 的代数域，这就是说，代数域这个性质是适合传递律的．

证明　假定 α 是 K 中元，$\alpha_0,\alpha_1,\cdots,\alpha_n$ 是 $L[x]$中 α 适合的既约多项式的系数，因为 L 是 F 的代数域，所以 α_i 是 F 的代数元．因此 $L'=F(\alpha_0,\alpha_1,\cdots,\alpha_n)$是 F 的有穷次域，于是 $L'(\alpha)$是 F 的有穷次域，所以 $L'(\alpha)$是 F 的代数域，因此 α 是 F 的代数元，定理成立．

假定 K 是 F 的扩张域，那么 K 中 F 的所有代数元成为一子域，我们用 L 来表示．显然，它是 K、F 的中间体．并且是 K 中 F 的**最大代数域**，这时 K 中除 L 的元外，任意元都是 L 的超越元．这是因为，假如 α 是 K 中 L 的代数元，那么 $L(\alpha)$是 L 的代数扩张域．因为 L 是 F 的代数扩张域，所以 $L(\alpha)$也是 F 的代数扩张域，于是 α 是 F 的代数元，因此 $\alpha\in L$. 如这样的 L 扩张体，其中除 L 中元外，任意元都是 L 的超越元时，叫做 L 的**纯超越扩张体**，或者叫做 L 的**纯超越体**．因此域 K 可以先从 F 代数扩张到 L，再从 L 纯超越扩张而成．也就是说，任意扩张可以由先代数扩张再超越扩张而成．

习　题　5.4

1. 假定 R 是有单位元的整环，S 是 R 的子环，并且包含它的单位元，如果 R 中任意元都是 S 的代数整元（满足首项系数是单位元的多项式），那么

R,S 中有一是体．它一也是体．

2. 假定 K 是有理数域 Q 的 2 次代数体，试证 $K=Q(\sqrt{a})$，这里 a 是没有相同的质因数的整数，并且当 $a\neq b$ 时，$Q(\sqrt{a})\neq Q(\sqrt{b})$.

§5.5 分裂域、正规扩张域

我们知道，域 F 的代数域 K 中元都是 $F[x]$ 中多项式的零点，所以 K 的某些性质可以由 $F[x]$ 中多项式的性质来确定，因此在讨论 K 时，我们可以从 $F[x]$ 中多项式入手．这节我们讨论 F 的两个特殊的代数扩张域，下节根据 $F[x]$ 中多项式零点的性质把 F 的代数体来分类．

由§5.3 我们知道，$F[x]$ 中任意多项式 $f(x)$ 在 F 的某扩张域 K 中含有它的零点．因此，在 $K[x]$ 中 $f(x)$ 有一次因式．这时我们也说它在 $K[x]$ 中**能够分裂**．假如 $f(x)$ 在 $K[x]$ 中能够分裂为一次因式的乘积，我们就说它在 K 中**能够完全分裂**．譬如，系数是复数的多项式在复数域中就能够完全分裂．

定义 1 假设 $f(x)$ 是 $F[x]$ 中多项式，K 是 F 的扩张域，如果在 K 中，$f(x)$ 能够完全分裂，即

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\ \alpha_i\in K,$$

但在 K、F 的任意异于 K 的中间体中(假如存在)，$f(x)$ 不能够完全分裂，那么 K 叫做 $f(x)$ 的**分裂域**．

譬如，Q 是有理数域，$f(x)=x^2-2$，因为在 $Q(\sqrt{2})$ 中，

$$f(x)=(x-\sqrt{2})(x+\sqrt{2}),$$

所以 $Q(\sqrt{2})$ 是 $f(x)$ 的分裂域．

假如 K 是 $F[x]$ 中 $f(x)$ 的分裂域，那么 K 就是由 F 添加 $f(x)$ 在 K 中所有零点 $\alpha_1,\cdots,\alpha_n$ 形成的域．即 $K=F(\alpha_1,\cdots,\alpha_n)$．因此 K 是 F 的有穷次代数域．

定理 1 $F[x]$ 中任意多项式 $f(x)$ 有分裂域．

证明 假设 $f(x)$ 在 $F[x]$ 中分裂为既约多项式 $f_i(x)$ 的乘积：

$$f(x)=f_1(x)f_2(x)\cdots f_{m_1}(x),$$

如果 $f_i(x)$ 都是1次，那么 F 就是 $f(x)$ 的分裂域，如果 $f_i(x)$ 的次数不都是1，假如 $f_1(x)$ 的次数大于1，我们把 $f_1(x)$ 的一零点 α_1 添加于 F 得到 $K_1=F(\alpha_1)$，在 $K_1[x]$ 中，$f(x)$ 最少有一个1次因式 $x-\alpha_1$，因此 $f(x)$ 能够分裂为1次因式 $x-\alpha_1$ 及既约因式 $g_i(x)$ 的乘积，即

$$f(x)=(x-\alpha_1)g_1(x)\cdots g_{m_2}(x).$$

如果 $g_i(x)$ 都是1次，那么 K_1 就是 $f(x)$ 的分裂域；如果 $g_i(x)$ 不都是1次，重复引用上面的方法，因为 $f(x)$ 的次数是有穷，所以在 F 的扩张域中，$f(x)$ 的1次因式只能有穷多个，因此继续添加有穷个零点 α_i 后，我们得到域 $K_m=F(\alpha_1,\cdots,\alpha_m)$. 在 K_m 中，$f(x)$ 能够完全分裂，因此定理得证.

由上面的证明及§5.3，我们不难知道任意多项式的分裂域不是唯一的. 为了更好地说明它们之间的关系，我们先介绍下面一个基本概念.

定义2　假如体 $K,\overline{K}$ 分别是体 $F,\overline{F}$ 的扩张体，σ 是 $F,\overline{F}$ 的同构，τ 是 $K,\overline{K}$ 的同构，如果

$$\tau(a)=\sigma(a),a\in F,$$

也就是说，F 中任意元对于 σ,τ 的象都相同，那么 τ 叫做 σ 的延长，而 $K,\overline{K}$ 叫做 $F,\overline{F}$ 的延长.

当 $F=\overline{F}$，σ 是恒等映射时，τ 就是 $K,\overline{K}$ 关于 F 的同值，因此同值是延长的特例. 引用延长这个概念，我们得到下面比§5.3定理3更广泛的定理.

定理2　假如域 $F,\overline{F}$ 同构，$f(x)$ 是 $F[x]$ 中既约多项式，$\overline{f}(x)$ 是 $\overline{F}[x]$ 中与 $f(x)$ 对应的多项式(即系数分别是 $f(x)$ 中系数的象)，α 是 $f(x)$ 的零点，$\overline{\alpha}$ 是 $\overline{f}(x)$ 的零点，那么 $F(\alpha),\overline{F}(\overline{\alpha})$ 是 $F,\overline{F}$ 的延长.

证明　首先 $\overline{f}(x)$ 是 $\overline{F}[x]$ 中既约多项式. 这是因为，如果在

$\overline{F}[x]$中，$\overline{f}(x)$是可约的，$\overline{f}(x)=\overline{f}_1(x)\overline{f}_2(x)$，假定$f_1(x)$，$f_2(x)$是$F[x]$中分别与$\overline{f}_1(x)$，$\overline{f}_2(x)$对应的多项式，因为$F\simeq\overline{F}$，对于$\overline{F}$中任意两元的和及积的象源分别是它们的象源的和及积，所以$f(x)=f_1(x)f_2(x)$，这与$f(x)$是既约的假设不合．

再假设F，$\overline{F}$的同构把F中元a变成$\overline{F}$中元$\overline{a}$，$f(x)$的次数是n，那么$F(\alpha)$中任意元可以写成$\sum_{i=0}^{n-1}a_i\alpha^i$，$\overline{F}(\overline{\alpha})$中任意元可以写成$\sum_{i=0}^{n-1}\overline{a}_i\overline{\alpha}^i$，因此下面的对应$\sigma$：

$$g(\alpha)=\sum_{i=0}^{n-1}a_i\alpha^i\rightarrow\overline{g(\alpha)}=\sum_{i=0}^{n-1}\overline{a}_i\overline{\alpha}^i$$

显然是$F(\alpha)$射到$\overline{F}(\overline{\alpha})$上的映射，并且还是双射．如果我们能够证明$\sigma$是$F(\alpha)$到$\overline{F}(\overline{\alpha})$上的同构，因为$\sigma(a)=\overline{a}$，$a\in F$，于是$F(\alpha)$，$\overline{F}(\overline{\alpha})$是$F$，$\overline{F}$的延长，因此定理就告成立．

假定$h(\alpha)=\sum_{i=0}^{n-1}b_i\alpha^i$，因为

$$g(\alpha)+h(\alpha)=\sum_{i=0}^{n-1}(a_i+b_i)\alpha^i,\overline{a_i+b_i}=\overline{a}_i+\overline{b}_i,$$

所以$\overline{g(\alpha)+h(\alpha)}=\overline{g(\alpha)}+\overline{h(\alpha)}$．设

$$g(x)h(x)=q(x)f(x)+r(x),$$

因为对于F中任意元a，b，我们有$\overline{a+b}=\overline{a}+\overline{b}$，$\overline{ab}=\overline{a}\overline{b}$，因此

$$\overline{g}(x)\overline{h}(x)=\overline{q}(x)\overline{f}(x)+\overline{r}(x),$$

于是

$$g(\alpha)h(\alpha)=r(\alpha),\overline{g}(\overline{\alpha})\overline{h}(\overline{\alpha})=\overline{r}(\overline{\alpha}).$$

因为$r(\alpha)\rightarrow\overline{r}(\overline{\alpha})$，所以

$$\overline{g(\alpha)h(\alpha)}=\overline{g(\alpha)}\cdot\overline{h(\alpha)}.$$

这就是说，映射σ是$F(\alpha)$到$\overline{F}(\overline{\alpha})$上的同构，因此$F(\alpha)$，$\overline{F}(\overline{\alpha})$是$F$，$\overline{F}$的延长，所以定理成立．

现在来讨论分裂域间的关系．

定理3 假设F是域，$f(x)$是$F[x]$中多项式，K，$\overline{K}$是$f(x)$

的分裂域，那么 $K,\overline{K}$ 关于 F 同值，也就是说，任意多项式的分裂域除同值的外是唯一的．

证明 假设 $f(x)$ 在 $F[x]$ 中分裂为既约多项式 $f_i(x)$ 的乘积：

$$f(x)=f_1(x)f_2(x)\cdots f_m(x),$$

因为 $f(x)$ 在 $F[x]$ 的因子分解是唯一的，所以 $f(x)$ 的分裂域包含它的既约因式 $f_i(x)$ 的分裂域．假如 $f_i(x)$ 都是 1 次的，那么 F 就是 $f(x)$ 的分裂域，即 $F=K$，因此这时定理成立．假如 $f_i(x)$ 不都是 1 次，$f_1(x)$ 的次数大于 1，我们命 $\alpha_1,\bar{\alpha}_1$ 分别是 $K,\overline{K}$ 中 $f_1(x)$ 的零点，由 §5.3 定理 3，$F(\alpha_1),F(\bar{\alpha}_1)$ 关于 F 同值．假如 $F(\alpha_1)$ 是 $f(x)$ 的分裂域，那么 $F(\bar{\alpha}_1)$ 也就是 $\bar{f}(x)$ 的分裂域，因此这时定理成立．假如 $F(\alpha_1)$ 又不是 $f(x)$ 的分裂域，在 $F(\alpha_1)$ 中再将 $f(x)$ 分解为既约多项式的乘积

$$f(x)=(x-\alpha_1)g_1(x)\cdots g_l(x),$$

那么在 $F(\bar{\alpha}_1)$ 中，$f(x)=(x-\bar{\alpha}_1)\bar{g}_1(x)\cdots\bar{g}_l(x)$，

假如 $g_1(x)$ 的次数大于 1，$\alpha_2,\bar{\alpha}_2$ 分别是 $g_1(x),\bar{g}_1(x)$ 在 $K,\overline{K}$ 中零点，由定理 2，$F(\alpha_1,\alpha_2),F(\bar{\alpha}_1,\bar{\alpha}_2)$ 关于 F 同值，重复引用上面的方法，因为 $f(x)$ 的次数是有穷，而 K 是于 F 添加 $f(x)$ 在 K 中所有零点扩张的体，因此继续进行有穷回后，就得到 $K,\overline{K}$，显然它们关于 F 同值，所以定理得证．

由上面的证明我们又知道，假如 $K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，那么 $\overline{K}=F(\bar{\alpha}_1,\bar{\alpha}_2,\cdots,\bar{\alpha}_n)$，并且 $K,\overline{K}$ 有把 α_i 变成 $\bar{\alpha}_i$ 关于 F 的同值．

假如 $F[x]$ 中多项式 $f(x)$ 的分裂域 $K=F(\alpha_1,\cdots,\alpha_n)$ 及 $\overline{K}=F(\bar{\alpha}_1,\cdots,\bar{\alpha}_n)$ 在同一包含体中，那么 $K,\overline{K}$ 不只关于 F 是同值，而且是相等，这是因为在这包含体中，

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)=(x-\bar{\alpha}_1)\cdots(x-\bar{\alpha}_n),$$

根据 §3.9 定理 7，这两种分解除顺序外是一致的，因此 $K,\overline{K}$ 是由相同的元添加于 F 扩张的域，所以 $K=\overline{K}$.

由定理 3 的证明，我们还可以知道多项式在一分裂域中如果有 m 重零点，那么在任一分裂域中也同样有 m 重零点，零点的相

重数与分裂域的选择无关.

上面我们介绍了分裂域,现在我们来介绍另一类叫做正规域的代数扩张域.

我们知道在$f(x)$的分裂域中,$f(x)$当然能够完全分裂,此外还有无其它多项式也能够在其中完全分裂.

假定$K=F(\alpha_1,\cdots,\alpha_n)$是$F[x]$中多项式$f(x)$的分裂域,$\alpha_i$是$f(x)$的零点,$g(x)$是$F[x]$中既约多项式,它有一零点$\beta\in K$,如果$\beta'$是$g(x)$在$K$的扩张域中任意零点,下面我们来证明$\beta'\in K$,因此$g(x)$在$K$中也能够完全分裂.

我们知道$F(\beta),F(\beta')$关于F同值,并且存在着不使F中任意元变动而把β变为β'的同值映射. 假如我们把$f(x)$分别看成为$F(\beta)[x],F(\beta')[x]$中多项式,于$F(\beta),F(\beta')$各添加$f(x)$的零点$\alpha_1,\cdots,\alpha_n$,一再引用定理2,就容易得知

$$F(\beta)(\alpha_1,\cdots,\alpha_n)\simeq F(\beta')(\alpha_{i_1},\cdots,\alpha_{i_n})$$

并且它们是$F(\beta),F(\beta')$的延长,这延长把α_k又变为α_{i_k}即$\alpha_1,\cdots,\alpha_n$仍然变为$\alpha_1,\cdots,\alpha_n$,只是它们间的顺序可能有所不同而已. 因为K是F的代数域,而β是K中元,所以β是系数为F中元的$\alpha_1,\cdots,\alpha_n$的多项式

$$\beta=h(\alpha_1,\cdots,\alpha_n).$$

由$F(\beta),F(\beta')$的同值关系,得知β'也是系数为F中元的$\alpha_1,\cdots,\alpha_n$的多项式,因此$\beta'\in F(\alpha_1,\cdots,\alpha_n)$,所以$g(x)$在$K$中完全分裂,这就是说,假如既约多项式$g(x)$在$f(x)$的分裂域$K$中能够分裂,那么它在$K$也能够完全分裂.

上面是分裂域的一个性质,F的任意代数域不一定都有这性质. 一般来说,我们有

定义3 假定域K是F的代数域,并且$F[x]$中任意既约多项式,如果在K中能够分裂,它在K中就能够完全分裂,那么K叫做F的**正规扩张域**,或简称F的**正规域**,有时又叫做F的**伽罗瓦域**.

于是我们得知，F 的代数域 K 是 F 的正规域的必要充分条件是 K 中任意元关于 F 的共轭元都在 K 中．这与§2.4中，群 G 的子群 H 是 G 的正规子群的必要充分条件是 H 中任意元的共轭元都在 H 中的性质一致，但要注意的是，这时 K 是 F 的扩张体，而 H 却是 G 的子群．

引用上面定义，由前面的讨论，我们有

定理 4 多项式环 $F[x]$ 中任意多项式 $f(x)$ 的分裂域是 F 的有穷次正规域．

因为 F 的代数域关于 F 不一定是有穷的，所以 F 的正规域关于 F 也不一定是有穷次的，譬如，上节中所有代数数组成的域是有理数体 Q 的正规域，它关于 Q 不是有穷次．在有穷次时，上面定理的逆定理也是成立的．

定理 5 假如 K 是 F 的有穷次正规域，那么 K 是 $F[x]$ 中某多项式的分裂域

证明 因为 K 关于 F 是有穷次的，所以 K 是添加其中有穷个元 $\alpha_1,\cdots,\alpha_n$ 于 F 形成的域，即

$$K=F(\alpha_1,\cdots,\alpha_n).$$

假设 $f_i(x)$ 是 $F[x]$ 中零点为 α_i 的既约多项式，因为 K 是 F 的正规域，所以 $f_i(x)$ 在 K 中完全分裂．于是 $f(x)=\prod_{i=1}^{n}f_i(x)$ 在 K 中也能够完全分裂，因此 K 是 $f(x)$ 的分裂域，所以定理得证．

显然，F 的有穷次扩张域 K 不一定是 F 的正规域，但是由上面的证明，我们可以再扩张 K 使它成为 F 的正规域，也就是说，在 F 的扩张域中有包含 K 的正规域．

添加 $F[x]$ 的既约多项式 $f(x)$ 的一个零点 α 于 F 所得到的域 $F(\alpha)$ 一般不一定是 $f(x)$ 的分裂域，因此也不一定是 F 的正规域．如果 $F(\alpha)$ 是 F 的正规域，这时多项式 $f(x)$ 叫做 F 的**正规式**或者叫做**伽罗瓦式**．显然 2 次既约多项式是正规式．

下面，我们来介绍正规域的一些基本性质，这些性质与§2.4

中关于正规子群的非常类似.

由§2.4我们得知,H是群G的正规子群的必要充分条件是H与它的共轭子群相等,与这类似,我们有

定理6 假如α是$F[x]$中既约多项式$f(x)$在它的分裂域K的零点,α_i是K中$f(x)$的任意零点,那么$F(\alpha)$是F的正规域的必要充分条件是$F(\alpha)$与它关于F的任意共轭体$F(\alpha_i)$相等,即

$$F(\alpha)=F(\alpha_i).$$

证明 假如$F(\alpha_i)=F(\alpha)$,那么$F(\alpha)$就是$f(x)$的分裂域,所以$F(\alpha)$是F的正规域. 反过来,假如$F(\alpha)$是F的正规域,因为α_i是$f(x)$的零点,所以$\alpha_i\in F(\alpha)$,因此$F(\alpha_i)\subseteq F(\alpha)$,但$(F(\alpha):F)=(F(\alpha_i):F)$,所以$(F(\alpha):F(\alpha_i))=1$,于是$F(\alpha_i)=F(\alpha)$. 因此定理成立.

再我们还有

定理7 假定$K\supseteq L\supseteq F$,并且K是F的正规域,那么K也是L的正规域.

证明 因为K是F的正规域,所以K是F的代数域,因此K也是L的代数域. 再假如$f(x)$是$L[x]$中既约多项式,α是它在K中一零点,$g(x)$是$F[x]$中零点为α的既约多项式,由§5.3习题6,我们得知$f(x)$是$g(x)$的因式. 因为$g(x)$在K中能够完全分裂,所以$f(x)$在K中也能够完全分裂,因此K是L的正规域,于是定理成立.

同群的情况一样,要注意的是,在上面定理中,虽然K是F的正规域,但L不一定是F的正规域. 譬如Q是有理数域,ω是1的虚立方根,那么

$$Q(\sqrt[3]{2},\omega)\supset Q(\omega\sqrt[3]{2})\supset Q,$$

这时$Q(\sqrt[3]{2},\omega)$是多项式x^3-2的分裂域,所以它是Q的正规域,但$Q(\omega\sqrt[3]{2})$不是Q的正规域.

此外,还要注意的是,如果K是L的正规域,L是F的正规域,那么K也不一定是F的正规域. 这就是说,正规域这个关系

是不适合传递律的．譬如 Q 是有理数域，因为

$$Q(\sqrt[4]{2})\supset Q(\sqrt{2})\supset Q,$$

显然，$Q(\sqrt[4]{2})$ 是 $Q(\sqrt{2})$ 的正规域，$Q(\sqrt{2})$ 是 Q 的正规域，但 $Q(\sqrt[4]{2})$ 不是 Q 的正规域．

习 题 5.5

1. 试求多项式 x^3-x^2-x-2 关于有理数域的分裂域．
2. 试证多项式 x^4+4x^2+2 是有理数域的正规式．
3. 试证 F 的 2 次体是 F 的正规域．
4. 试证 $F[x]$ 中 n 次多项式的分裂域关于 F 的次数不能大于 $n!$
5. 假如把 $F[x]$ 中无穷多个多项式的零点都添加于 F，得到的域也是 F 的正规域，如何证明？
6. 试证整系数 3 次多项式成为有理数域的正规式的必要充分条件是它的判别式是有理数的平方．

§5.6 可离扩张域、不可离扩张域

代数扩张体与它所添加的代数元有关，而代数元又与它适合的既约多项式有关，但既约多项式有的有重零点，有的没有重零点，这节我们就这两种情形来讨论代数域的构造．

我们知道，在中学代数中既约多项式是没有重零点的，如果 F 是任意域，$F[x]$ 中既约多项式 $f(x)$ 能否有重零点？因为多项式零点的重数与它的分裂域的选取无关，因此，在讨论这问题时，我们就可以不考虑它所在的分裂域．

由§3.10 得知，$f(x)$ 有重零点的必要充分条件是 $f(x)$ 与 $f'(x)$ 有次数大于零的公因式，但既约多项式的因式只有常数及自身，因此既约多项式 $f(x)$ 有重零点的必要充分条件是 $f(x)$ 能够整除 $f'(x)$ 即 $f(x)\mid f'(x)$，也就是 $f'(x)=0$.

假设既约多项式 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$，如果 $f'(x)=\sum\limits_{i=1}^{n}ia_ix^{i-1}=0$，

那么

$$ia_i=0,i=1,\cdots,n.$$

当 F 的特征数是零时，我们有

$$a_i=0,i=1,\cdots,n.$$

于是 $f(x)=a_0$，因此 $f(x)$ 是 $F[x]$ 中可逆元，这与 $f(x)$ 是既约的假设不合，所以 $f'(x)\neq 0$. 于是，这时既约多项式 $f(x)$ 没有重零点. 当 F 的特征数是 p 时，如果 $i\not\equiv 0(p)$，我们就有

$$a_i=0,$$

因此
$$f(x)=a_0+a_px^p+a_{2p}x^{2p}+\cdots,$$

也就是说，这时 $f(x)$ 是 x^p 的多项式. 反过来，如果 $f(x)$ 是 x^p 的多项式，那么 $f'(x)=0$，因此它有重零点. 于是，我们有

定理 1 域 F 的特征数如果是零，那么 $F[x]$ 中既约多项式没有重零点；如果是 p，那么 $F[x]$ 中既约多项式有重零点的必要充分条件是：它是 x^p 的多项式.

于是，在特征数是 p 的域中，既约多项式有的是有重零点的. 但是有重零点的，它的零点是否都是重零点？

假设既约多项式 $f(x)$ 是 x^p 的多项式，我们把它写成 $f(x)=h(x^p)$. 如果 $h(x)$ 又是 x^p 的多项式，那么 $f(x)$ 就是 x^{p^2} 的多项式. 现在假定 $f(x)$ 是 x^{p^k} 的多项式而不是 $x^{p^{k+1}}$ 的多项式，我们用

$$f(x)=g(x^{p^k})$$

来表示. 因为 $f(x)$ 是既约的，所以 $g(x)$ 也是既约的. 再假如 $g'(x)=0$，那么 $g(x)$ 又是 x^p 的多项式，因此 $f(x)$ 就是 $x^{p^{k+1}}$ 的多项式了，这与假设不合. 于是 $g'(x)\neq 0$，所以这时的既约多项式 $g(x)$ 没有重零点.

假定 $g(y)$ 的次数是 n_0，首项系数是 1（F 的单位元），在它的分裂体中，它分裂为 1 次因式 $y-\beta_i$ 的乘积，即

$$g(y)=\prod_{i=1}^{n_0}(y_i-\beta_i),$$

因此
$$f(x)=\prod_{i=1}^{n_0}(x^{p^k}-\beta_i).$$
如果 α_i 是 $x^{p^k}-\beta_i$ 的零点，也就是说 $\alpha_i^{p^k}=\beta_i$，那么
$$x^{p^k}-\beta_i=x^{p^k}-\alpha_i^{p^k}=(x-\alpha_i)^{p^k}.$$
于是
$$f(x)=\prod_{i=1}^{n_0}(x-\alpha_i)^{p^k}.$$
所以 $f(x)$ 有 n_0 个互异的零点 $\alpha_1,\cdots,\alpha_n$，并且它们都是 p^k 重零点．因此我们有

定理 2 假定域 F 的特征数是 p，$F[x]$ 中既约多项式 $f(x)$ 有重零点，那么 $f(x)$ 的零点都是重零点，并且有相同的重数 p^k.

上面 $g(y)$ 的次数 n_0 是既约多项式 $f(x)$ 互异零点的个数，叫做 $f(x)$（或 α_i）的**缩减次数**．p^k 是 $f(x)$ 零点的**重数**，k 叫做 $f(x)$（或 α_i）关于 F 的**指数**．显然，$f(x)$ 的次数 n，缩减次数 n_0 及指数 k 之间有如下关系：

(1) $$n=n_0p^k.$$

$F[x]$ 中多项式 $f(x)$ 如果没有重零点，就叫做 F 的**可离多项式**，否则就叫做 F 的**不可离多项式**．可离既约多项式的零点叫做**可离元**，不可离既约多项式的零点叫做**不可离元**．F 中元显然是 F 的可离元．当 F 的特征数是零时，它的既约多项式都是可离的，因此 F 的代数元都是可离元．当 F 的特征数是 p 时，指数是零的既约多项式是可离的，既约多项式是不可离的必要充分条件是它是 x^p 的多项式．

特别当 $n_0=1$ 时，既约多项式 $f(x)=x^{p^k}-\beta$ 叫做 $F[x]$ 的**纯不可离多项式**，它的零点 α，叫做 F 的**纯不可离元**，这时 $\alpha^{p^k}\in F$，但 $\alpha^{p^{k-1}}\overline{\in}F$. 反过来，假如 $\alpha^{p^k}\in F$，但 $\alpha^{p^{k-1}}\overline{\in}F$，这里 p 是 F 的特征数，那么
$$f(x)=x^{p^k}-\alpha^{p^k}=(x-\alpha)^{p^k}$$
在 $F[x]$ 中是既约的．因此 α 是 F 的纯不可离元，这是因为，如果

它是可约的，$g(x)$是它的既约因式，因为零点重数是 p 的幂，所以 $g(x)=(x-\alpha)^{p^l}$，$l<k$，于是 $\alpha^{p^l}\in F$，这与 $\alpha^{p^{k-1}}\overline{\in}F$ 的假设不合，因此 $f(x)$是既约的．

下面是可离元、不可离元的基本性质．

定理 3 假定域 F 的特征数是 p，α 是 F 的可离元，那么 α^p 也是可离元．

证明 假定可离元 α 适合的既约多项式 $f(x)=\sum_{i=0}^{n}a_ix^i$，

$$g(x)=\sum_{i=0}^{n}a_i^px^i$$

因为
$$g(\alpha^p)=\sum a_i^p\alpha^{ip}=(\sum a_i\alpha^i)^p=0.$$

只要 $g(x)$是可离既约多项式，那么 α^p 就是可离元了．

假定 $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$的零点，因为 $\alpha_i^p-\alpha_j^p=(\alpha_i-\alpha_j)^p\neq0$，所以 $g(x)$的零点 $\alpha_1^p,\cdots,\alpha_n^p$ 互异，因此 $g(x)$是可离多项式．再如果 $h(x)$是 $F[x]$中 $g(x)$的既约因式，$h(\alpha_k^p)=0$，所以 $h(x^p)$与 $f(x)$有公共零点 α_k，于是 $f(x)|h(x^p)$，因此，$h(\alpha_i^p)=0$，$i=1,\cdots,n$. 所以 $g(x)=h(x)$，即 $g(x)$是既约多项式．证明完毕．

于是假如 α 是 F 的可离元，那么 α^{p^r}也是可离元，由后面定理 9 我们还得知 α 的任意乘幂 α^r 都是可离元．

定理 4 假定域 F 的特征数是 p，α 是 F 的不可离元，

$$0<r\not\equiv0(p),$$

那么 α^r 也是不可离元．

证明 用反证法，假定 α^r 是可离元，它适合的既约多项式 $g(y)\in F[y]$没有重零点，设

$$g(y)=(y-\beta_1)\cdots(y-\beta_n),\beta_i\neq\beta_j,i\neq j.$$

于是 $g(x^r)=(x^r-\beta_1)\cdots(x^r-\beta_n)$也没有重零点，因为 $g_i(x)=x^r-\beta_i$ 与 $g'_i(x)=rx^{r-1}$没有公因式，从而 $g_i(x)$没有重零点．再假定 $f(x)$是 $F[x]$中 α 适合的既约多项式，因为 α 也适合 $g(x^r)$，所以 $f(x)|g(x^r)$，即

$$g(x^r)=f(x)\cdot h(x).$$

因为 $f(x)$ 有重零点，这与 $g(x^r)$ 没有重零点矛盾，所以 α^r 是不可离元.

定理证毕.

于是，假如 α 是不可离元，那么 $\alpha,\alpha^2,\cdots,\alpha^{p-1}$ 也都是不可离元.

定理5 假定域 F 的特征数是 p，α 是指数为 k 的 F 的不可离元，那么 α^{p^r} 当 $1\leqslant r\leqslant k-1$ 时，仍然是 F 的不可离元，但当 $r\geqslant k$ 时，就是 F 的可离元. 也就是说，不可离元 α 的指数 k 是使 α^{p^k} 成为可离元的最小正整数.

证明 假定 $f(x)=g(x^{p^k})$ 是 $F[x]$ 中 α 适合的既约多项式，那么 $g(\alpha^{p^k})=0$，因为 $g(x)$ 是可离多项式，所以 α^{p^k} 是可离元. 再由定理3，显然定理的后半段成立.

再当 $1\leqslant r<k$ 的时候，α^{p^r} 适合 $g(x^{p^{k-r}})$，因为 $g(x^{p^k})$ 是既约的，所以 $g(x^{p^{k-r}})$ 也是既约的. 又因为 $g(x^{p^{k-r}})$ 是 x^p 的多项式，所以 $g(x^{p^{k-r}})$ 是不可离多项式，因此 α^{p^r} 是不可离元. 于是定理的前半段成立.

定理证毕.

上面是介绍可离多项式、不可离多项式、可离元、不可离元等概念及它们的基本性质，现在我们引用它来讨论代数域的构造.

域 F 的代数域，如果其中任意元是 F 的可离元，就叫做 F 的**可离域**，否则就叫做 F 的**不可离域**. 特别，域 F，如果它的任意代数元都是 F 的可离元，也就是说，如果 $F[x]$ 中任意既约多项式都是 F 的可离多项式时，叫做**完全域**，否则叫做**不完全域**. 显然，特征数是零的域是完全域，完全域的代数域是这完全域的可离域. 根据定义，我们不难证明有穷体也是完全域，在代数域中，可离域是重要的一类，并且常常引用的域很多都是属于这类.

我们容易知道，由不可离元扩张的域显然是不可离域，但是由可离元扩张的域是否就是可离域？直接用定义来说明非常麻烦，下

面我们根据映射的个数(定理8)这个重要性质,来解答这问题.

假设α是$F[x]$中既约多项式$f(x)$在$L=F(\alpha)$中的零点,如果$f(x)$的缩减次数是n_0,那么$f(x)$在它的分裂域$K\supseteq L$中有互异的n_0个零点,因此L在K中有n_0个互异的同值映射,但是在K或K的扩张体中,L的互异同值映射是否只有这n_0个?

定理6 假设α是关于域F缩减次数为n_0的元,那么适当选取$F(\alpha)$的扩张体,在其中$F(\alpha)$关于F的同值映射能有n_0个互异的.但不论$F(\alpha)$的扩张体如何选取,在其中,$F(\alpha)$关于F的互异同值映射不能多于n_0个.

证明 假定$f(x)$是$F[x]$中α适合的既约多项式,如果$F(\alpha)$的扩张体选取$f(x)$的分裂体,显然在其中$F(\alpha)$就有n_0个互异的同值映射.但在$F(\alpha)$的任意扩张体中,$F(\alpha)$关于F的任意同值映射把α变为同一既约多项式$f(x)$的零点α_k,因此把$F(\alpha)$中任意元$\sum a_i\alpha^i$变为$\sum a_i\alpha_k^i$,也就是说,把$F(\alpha)$射到$F(\alpha_k)$,这映射就是上面n_0个同值映射中把α变为α_k的同值映射,所以$F(\alpha)$在它的任意扩张体中关于F互异的同值映射不能有多于n_0个,因此定理成立.

假定在$F(\alpha)$的适当扩张体中,$F(\alpha)$关于F互异同值映射的个数等于体的次数$(F(\alpha):F)$,显然α是F的可离元,因此,在$F(\alpha)$的适当扩张体中,$F(\alpha)$有$(F(\alpha):F)$个关于F的互异同值映射的必要充分条件是:α是F的可离元.

特别,假如α是F的纯不可离元,因为这时$n_0=1$,所以在$F(\alpha)$的任意扩张体中,$F(\alpha)$关于F的同值映射只有1个,那就是不动映射.反过来,假如在$F(\alpha)$的任意扩张体中,$F(\alpha)$关于F的同值映射只有1个,那么α就是F的纯不可离元.因此,在$F(\alpha)$的扩张体中$F(\alpha)$只有1个同值映射的必要充分条件是α是F的纯不可离元.

下面是一般情况.

定理7 假设$K=F(\alpha_1,\cdots,\alpha_m)$,$\alpha_i$是关于

$$F_{i-1}=F(\alpha_1,\cdots,\alpha_{i-1})$$

的缩减次数为 n_i 的元，$i=1,\cdots,m$，那么适当选取 K 的扩张体，在其中，K 关于 F 的互异同值映射有 $\prod_{i=1}^{m} n_i$ 个．但不论 K 的扩张体如何选，在其中 K 关于 F 的互异同值映射不能多于 $\prod_{i=1}^{m} n_i$ 个．

证明　就元 α 的个数用归纳法证明．当元数 $=1$ 时就是上面的定理 6，这时定理成立．假定元数 $=m-1$ 时定理成立：在 F_{m-1} 的适当扩张体中，F_{m-1} 关于 F 的互异同值映射有 $\prod_{i=1}^{m-1} n_i$ 个，但无论如何不能比这多．因为 K 关于 F 的任一同值映射产生 F_{m-1} 关于 F 的一个同值映射，因此 K 关于 F 的任一同值映射可以看成为 F_{m-1} 关于 F 的同值映射的延长．现在命 $\overline{F}_{m-1}$ 是 F_{m-1} 在 K 的适当扩张体中的一个同值象，$f(x)$ 是 $F_{m-1}[x]$ 中 α_m 适合的既约多项式，$\bar{f}(x)$ 是 $\overline{F}_{m-1}[x]$ 中与 $f(x)$ 对应的多项式，$\bar{\alpha}_m$ 是在 $\overline{F}_{m-1}$ 的适当扩张体中 $\bar{f}(x)$ 的任意一个零点．因为 $F_{m-1}\simeq\overline{F}_{m-1}$，所以

$$F_{m-1}(\alpha_m)\simeq\overline{F}_{m-1}(\bar{\alpha}_m),$$

也就是说 $K\simeq\overline{F}_{m-1}(\bar{\alpha}_m)$，因此对于 F_{m-1} 的一个同值映射我们有 n_m 个如此的延长，但无论如何不能比这多．于是在 K 的适当扩张体中，K 关于 F 的互异同值映射有

$$\prod_{i=1}^{m-1} n_i\cdot n_m=\prod_{i=1}^{m} n_i$$

个，但无论如何不能比这多，因此定理成立．

于是我们得知，假如 $K=F(\alpha_1,\cdots,\alpha_m)$ 是 F 的代数体，那么在 K 的任意扩张体中，K 关于 F 的互异同值映射不能多于 $(K:F)$ 个．当每个 α_i 是 $F_{i-1}=F(\alpha_1,\cdots,\alpha_{i-1})$ 的可离元时，K 关于 F 的互异同值映射才有 $(K:F)$ 个．

定理 8　在 $K=F(\alpha_1,\cdots,\alpha_m)$ 的适当扩张体中，K 有 $(K:F)$ 个关于 F 的互异同值映射的必要充分条件是：α_i 是

$$F_{i-1}=F(\alpha_1,\cdots,\alpha_{i-1}),i=1,\cdots,m$$

的可离元．

证明 条件的充分性很显然，今只用归纳法来证明必要性．

我们知道，K 关于 F 的任意同值映射可以看成是 F_{m-1} 关于 F 的同值映射的延长．根据假设，在 K 的适当扩张体中，K 关于 F 的同值映射有 $(K:F)$ 个，于是 F_{m-1} 关于 F 的同值映射有 $(F_{m-1}:F)$ 个，并且 F_{m-1} 关于 F 的任意同值映射有 $(K:F_{m-1})$ 个延长成为 K 关于 F 的同值映射，因为不这样，K 关于 F 的同值映射就不能有 $(K:F)$ 个，这与假设不合．因此由归纳法假设，α_i 是 F_{i-1} 的可离元，所以条件的必要性成立，因此定理得证．

要注意的是，K 关于 F 互异的同值映射的个数是 K 的内在性质，它与 α_i 的选择无关．现在我们来讨论上面提出的问题．

定理 9 假设 $K=F(\alpha_1,\cdots,\alpha_m)$，$\alpha_i$ 是 $F_{i-1}=F(\alpha_1,\cdots,\alpha_{i-1})$，$i=1,\cdots,m$ 的可离元，那么 K 是 F 的可离域．

证明 由定理 8 的充分条件，我们得知在适当扩张体中，K 关于 F 的互异同值映射有 $(K:F)$ 个．假定 $\beta(=\beta_1)$ 是 K 中任意元，我们可以适当地选取 β_i 使 $K=F(\beta_1,\beta_2,\cdots,\beta_k)$，根据定理 8 的必要条件，$\beta$ 是 F 的可离元，因此定理成立．

假如 α_i 是 F 的可离元，显然它也是 F_{i-1} 的可离元，因此，如果 $\alpha_1,\cdots,\alpha_m$ 都是 F 的可离元，那么 $F(\alpha_1,\cdots,\alpha_m)$ 是 F 的可离域，这就是说，由可离元扩张的域是可离域．于是在 F 的代数域 K 中，F 的可离元的和，差，积，商仍然是 F 的可离元．

在 § 5.4 中，我们知道代数域这个关系是适合传递律的，可离域这关系也适合传递律，即

定理 10 假如 K 是 L 的可离域，L 是 F 的可离域，那么 K 是 F 的可离域

证明 因为 K 中任意元 α 是 L 的可离元，假定 $\alpha_1,\cdots,\alpha_n$ 是 $L[x]$ 中 α 适合的既约多项式的系数，因为它们都是 F 的可离元，所以 $F(\alpha_1,\cdots,\alpha_n)$ 是 F 的可离域，再 α 显然是 $F(\alpha_1,\cdots,\alpha_n)$ 的可离

元，由定理 9，$F(\alpha_1,\cdots,\alpha_n,\alpha)$是 F 的可离域，所以 α 是 F 的可离元，因此定理得证．

假如 K 是 F 的代数域，那么在 K 中，所有 F 的可离元成为一子域 L，显然，L 是 K、F 的中间体，并且它是 K 中 F 的**最大可离域**，$(L:F)$叫做 K 关于 F 的**缩减次数**．我们容易得知，K 是 F 的可离域的必要充分条件是：K 关于 F 的次数$(K:F)$等于 K 关于 F 的缩减次数$(L:F)$，即$(K:F)=(L:F)$．由定理 10，我们容易得知 K 中除 L 中元外，任意元都是 L 的不可离元，也就是说，K 中 L 的可离元都在 L 中，如 K 这样的 L 扩张域，其中除 L 元外，任意元都是 L 的不可离元，叫做 L 的**纯不可离域**．再 K 中关于 L 的不可离元都是 L 的纯不可离元，这是因为假如 α 是 K 中指数为 k 的不可离元，那么 α^{p^k}是 L 的可离元，因此 $\alpha^{p^k}\in L$，所以 α 是 L 的纯不可离元，即纯不可离域中不可离元都是纯不可离元．于是代数扩张可以由先可离扩张、再纯不可离扩张而成．

假如 F 的代数域 K 中元关于 F 的指数有最大数，那么，这最大指数，我们又叫做 K 关于 F 的**指数**．下面来讨论 K 关于 F 的次数、缩减次数及指数间的关系．

假定域 F 的特征数是 p，$K=F(\alpha)$，如果 α 关于 F 的指数是 k，那么 K 关于 F 的指数就是 k．这是因为，K 中任意元可以写成 $\sum a_i\alpha^i$，由于 a_i 及 α^{p^k}都是 F 的可离元，所以

$$\left(\sum a_i\alpha^i\right)^{p^k}=\sum a_i^{p^k}\left(\alpha^{p^k}\right)^i$$

也是 F 的可离元，于是 $\sum a_i\alpha^i$ 关于 F 的指数不大于 k，因此，K 关于 F 的指数就是 k．假如 K 中 F 的最大可离域是 L，因为 α 是 L 的纯不可离元，所以 $x^{p^k}-\alpha^{p^k}$在 $L[x]$中是既约的．因此$(L(\alpha):L)=p^k$，但 $K=F(\alpha)=L(\alpha)$，所以$(K:L)=p^k$．于是

$$(K:F)=(K:L)(L:F)=(L:F)p^k.$$

再设 α 适合的 $F[x]$中既约多项式 $f(x)=g(x^{p^k})$，$f(x)$的次数 $n=n_0p^k$．因此，由上面等式得$(L:F)=n_0$，所以

(2) $$(K:F)=n_0p^k.$$

这里 n_0 是 $f(x)$ 互异零点的个数，也是 K 关于 F 互异同值映射的个数，又因为 $g(\alpha^{p^k})=0$，所以 $(F(\alpha^{p^k}):F)=n_0$，因此 $L=F(\alpha^{p^k})$，式(2)与前面式(1)是一致的．

一般假如 $K=F(\alpha_1,\cdots,\alpha_n)$，$\alpha_i$ 关于 F 的指数是 k_i，显然 $k_1,\cdots,k_n$ 中最大数就是 K 关于 F 的指数．再因为 L 是 K 中 F 的最大可离域，那么 $(K:L)=p^f$，因此

(3) $$(K:F)=(L:F)p^f,f\geqslant k,$$

这里 k 是 K 关于 F 的指数．这是因为，$(L(\alpha_1):L)=p^{k_1}$，假如命 $L[x]$ 中既约多项式 $x^{p^{k_2}}-\alpha_2^{p^{k_2}}=(x-\alpha_2)^{p^{k_2}}$ 在 $L(\alpha_1)[x]$ 的既约因式是 $x^{p^{k_2'}}-\alpha_2^{p^{k_2'}}=(x-\alpha_2)^{p^{k_2'}}$，$k_2'\leqslant k_2$，那么 $(L(\alpha_1,\alpha_2):L(\alpha_1))=p^{k_2'}$，因此 $(L(\alpha_1,\alpha_2):L)=p^{k_1+k_2'}$．再这样继续地进行下去，最后我们有 $(K:L)=p^f$，这里 $f=k_1+k_2'+\cdots+k_n'$，显然 $f\geqslant k$．这里 K 关于 F 的缩减次数 $(L:K)$ 是 K 关于 F 互异同值映射的个数，并且 $L=F(\alpha_1^{p^{k_1}},\cdots,\alpha_n^{p^{k_n}})$．上面(3)是(2)的推广．

习 题 5.6

1．假定 F 是特征数 p 的域，x 是未定元，试证多项式 y^p-x 在 $F(x)[y]$ 中是既约的，并且 $F(x)$ 是 $F(x^{\frac{1}{p}})$ 的不可离域．

2．假如 α 关于 F 的指数是 $k(>0)$，那么 α^p 关于 F 的指数是 $k-1$.

3．两个可离元的乘积是可离元还是不可离元？一个可离元与一个不可离元的乘积是可离元还是不可离元？两个不可离元的乘积是可离元还是不可离元？

4．假如特征数 p 的域 K 中各元的 p 乘幂形成的域是 K^p，试证 K 是完全域的必要充分条件是 $K=K^p$.

5．试证任意完全域的代数域是完全域．任意不完全域的有穷次域是不完全域．

6．假如 K 是 F 的纯不可离域，试证 K 是 F 的正规域，并且在任一扩张体中，K 关于 F 的同值映射是恒等映射．

7. 假定 K 是 F 的代数扩张域，L 是 K 中 F 的最大可离域，试证 K 关于 F 同值映射的个数等于 K 关于 F 的缩减次数.

8. 假定 K 是 F 的代数域，$K \supseteq L \supseteq F$，$K$ 关于 L 的缩减次数是 m，L 关于 F 的缩减次数是 n，试证 K 关于 F 的缩减次数是 mn.

9. 假如 K 是 L 的纯不可离域，L 是 F 的纯不可离域，那么 K 是 F 的纯不可离域，这就是说，纯不可离这个关系也适合传递律.

10. 假如 $\alpha_1, \cdots, \alpha_n$ 是 F 的纯不可离元，试证 $F(\alpha_1, \cdots, \alpha_n)$ 是 F 的纯不可离域，即由纯不可离元扩张的域是纯不可离域.

§5.7　有穷次扩张域的单纯性

我们知道在扩张域中，单扩张是构造最简单的. 有的扩张域形状上虽然不是单扩张，但我们可以把它改写成单扩张，这样在讨论时很多问题就能够简化. 但是怎样的扩张域能够改写成单扩张?

我们容易得知，于 F 添加两个(无关的)超越元扩张的域不是 F 的单扩张，添加一个代数元及一个超越元扩张的域也不是 F 的单扩张. 此外，F 的无穷次代数域显然也不是 F 的单扩张，因此单扩张或者是本原元，只有在有穷次代数域中来讨论了.

假定 K 是 F 的有穷次代数域. 如果 F 只含有穷个元，那么 K 也只含有穷个元. 在下节中我们就知道，元数是有穷的域是有本原元的，因此在这节我们假定 F 含无穷个元.

下面是单扩张的一个充分条件.

定理 1　假如 $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 F 的有穷次代数域，$\alpha_2, \cdots, \alpha_n$ 是 F 的可离元，那么 K 是 F 的单扩张域.

证明　我们用数学归纳法来证明. 当 $n=1$ 时，定理显然成立.

当 $n=2$ 时，为了方便起见，我们把 α_1, α_2 分别写成 α, β. 假定 $f(x), g(x)$ 是 $F[x]$ 中零点分别为 α, β 的既约多项式，并且在包含 $f(x), g(x)$ 的分裂域的扩张域中. 我们假定 $f(x)$ 的零点是 $\alpha_1 =$

$\alpha_1,\alpha_2,\cdots,\alpha_r$, $g(x)$的零点是$\beta_1=\beta,\beta_2,\cdots,\beta_s$. 因为$\beta\neq\beta_i$, $i\neq 1$, 所以对于任意i及$j(\neq 1)$, 多项式

$$\alpha_i+x\beta_j=\alpha+x\beta$$

在F中最多只有一个零点. 但F中含无穷个元, 因此F中有不适合这些式的元. 假如a是这样的一元, 即

$$\alpha_i+a\beta_j\neq\alpha+a\beta,\ j\neq 1.$$

命$\gamma=\alpha+a\beta$, 于是

$$F(\gamma)\subseteq F(\alpha,\beta).$$

如果我们能够证明$\beta\in F(\gamma)$, 那么$\alpha=\gamma-a\beta\in F(\gamma)$, 因此$F(\alpha,\beta)=F(\gamma)$, 于是$\gamma$就是所求的本原元了.

因为

$$g(\beta)=0,\ f(\alpha)=f(\gamma-a\beta)=0,$$

所以β是$F(\gamma)[x]$中多项式$g(x)$, $f(\gamma-ax)$的公共零点. 但当$j\neq 1$时, $\gamma-a\beta_j\neq\alpha_i$, 因此

$$f(\gamma-a\beta_j)\neq 0.$$

于是$g(x)$, $f(\gamma-ax)$在$F(\gamma)$的扩张域中只有一个公共零点β, 所以$g(x)$, $f(\gamma-ax)$只有一个1次公因式$x-\beta$, 也就是说, $x-\beta$是$g(x)$, $f(\gamma-ax)$的最大公因式. 再因为$g(x)$, $f(\gamma-ax)$的系数都在$F(\gamma)$中, 而两式的最大公因式可以用欧氏法式求得, 因此它们最大公因式的系数也都在$F(\gamma)$中, 于是$\beta\in F(\gamma)$, 所以$n=2$时定理成立.

假如在$n-1$时定理成立, 命$F(\alpha_1,\cdots,\alpha_{n-1})=F(\alpha)$, 那么

$$F(\alpha_1,\cdots,\alpha_{n-1},\alpha_n)=F(\alpha,\alpha_n)=F(\gamma),$$

这就是说在n时定理成立, 因此定理得证.

譬如$Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2}+\sqrt{3})$, 其中$Q$是有理数域, 这性质我们也可这样来验证, 因为$\gamma=\sqrt{2}+\sqrt{3}$, $\gamma^3=11\sqrt{2}+9\sqrt{3}$, 所以$\sqrt{2}$, $\sqrt{3}$都能够用γ的多项式表出.

1967年, 桑(J. Sonn)与查生浩斯(H. Zassenhaus, 1912～)给出一个不分F是有穷域或无穷域的证明[7], 读者可以参考.

于是，我们得知有穷次可离域是单扩张域，特征数是零的有穷次域也是单扩张域．对于特征数是 p 的有穷次域，我们有

定理 2 假定域 F 的特征数是 p，K 是 F 的 n 次代数域，那么，K 是 F 的单扩张域的必要充分条件是

$$n=n_0p^k,$$

这里 n_0 及 k 分别是 K 关于 F 的缩减次数及指数．

证明 假定 K 是 F 的单扩张域，$K=F(\alpha)$，k 是 α 关于 F 的指数，也就是 K 关于 F 的指数，L 是 K 中 F 的最大可离域，由§5.6 中的(2)式，我们有 $n=n_0p^k$，因此条件的必要性成立．

反过来，假定 $n=n_0p^k$，因为 L 是 F 的有穷次可离域，所以它是 F 的单扩张域，我们命 $L=F(\alpha)$．再假定 β 是 K 中关于 F 指数为 k 的元，那么 $(L(\beta):L)=p^k$，因此 $(L(\beta):F)=(L(\beta):L)\cdot(L:F)=n_0p^k$，于是 $K=L(\beta)$，所以 $K=F(\alpha,\beta)$．但 α 是 F 的可离元，由定理 1，K 有关于 F 的本原元，这就是说，K 是 F 的单扩张域，所以条件的充分性成立，因此定理得证．

关于单扩张还有下面斯太尼兹给出的必要充分条件．

定理 3 假定 K 是 F 的有穷次域，那么 K 是 F 的单扩张的必要充分条件是 K、F 的中间体只有有穷个[8]．

证明 假定 $K=F(\alpha)$，F_1 是 K,F 的中间体，即 $K\supseteq F_1\supseteq F$，$f(x)$，$g(x)$ 分别是在 $F[x]$，$F_1[x]$ 中 α 适合的既约多项式，那么 $g(x)\mid f(x)$．

今设 $g(x)=\sum_{i=0}^{n}a_ix^i$，$F(a_0,\cdots,a_n)=F_2$，显然 $F\subseteq F_2\subseteq F_1$，因此 $g(x)$ 在 $F_2[x]$ 中也是既约的．由于 $K=F_1(\alpha)$，$K=F_2(\alpha)$，所以 $(K:F_1)=(K:F_2)$，于是 F_2 等于 F_1，这就是说，F_1 由 $f(x)$ 的因式 $g(x)$ 完全决定，但 $f(x)$ 在 $K[x]$ 中只有有穷个因子，因此 K、F 的中间体只有有穷个，必要条件成立．

再假如 K、F 的中间体只有有穷个，同定理 1 的证明类似，对于 K 中任意元 α,β 如果能找到 v 使

$$F(\alpha,\beta)=F(v).$$

那么 K 就是 F 的单扩张域了. 设 $v=\alpha+a\beta,a\in F$,因为 F 含无穷多个元,而 $F(v)$ 只有有穷个,所以有 $v_1=\alpha+a_1\beta,v_2=\alpha+a_2\beta,a_1\neq a_2$ 使 $F(v_1)=F(v_2)$. 因为 $v_1,v_2\in F(v_1)$,所以 $v_1-v_2=(a_1-a_2)\beta\in F(v_1)$,因此 $\beta\in F(v_1)$,于是 $v_1-a\beta=\alpha\in F(v_1)$,即 $F(\alpha,\beta)\subseteq F(v_1)$. 所以 $F(\alpha,\beta)=F(v)$. 充分条件成立.

定理证毕.

下面是关于单扩张中间体的一个重要性质.

定理 4 假定 $F(\alpha)$是 F 的代数域,K 是 $F(\alpha)$,F 的中间体,那么 K 是 F 的单扩张域.

证明 因为$F(\alpha)$是F 的代数域,所以$F(\alpha)$是F 的有穷次域,由定理 3 的必要条件,$F(\alpha)$、F 的中间体只有有穷个. 现设 K 是 $F(\alpha)$、F 的中间体,那么 K、F 的中间体也是 $F(\alpha)$,F 的中间体,因此K、F 的中间体也只有有穷个. 于是由定理 3 的充分条件,K 是 F 的单扩张域.

定理证毕.

习 题 5.7

1. 试求 $Q(\sqrt{3},\sqrt[3]{2})$的本原元,这里 Q 是有理数域.

2. 试求 $Q(i,\sqrt{2})$的本原元.

3. 假如 x,y 是未定元,试证 $F(x,y)$的扩张域 $F(x^{\frac{1}{p}},y^{\frac{1}{p}})$没有本原元,这里 p 是 F 的特征数.

§5.8 有 穷 体

我们知道,元数是有穷的体叫做有穷体,这节我们讨论有穷体的构造.

假设 K 是有穷体,显然它包含的质域 F 也是有穷体,因为特征数是零的质域与有理数域同构,它不是有穷体. 所以 K 的特征

数异于零．我们假定 K 的特征数是 p．

再因为 K 只含有穷个元，显然其中关于 F 线性无关的元也只能是有穷个，因此 K 关于 F 是有穷次．假如 $(K:F)=n$，$\alpha_1,\cdots,\alpha_n$ 是 K 关于 F 的底，那么 K 中任意元能够唯一地表成下面形状：

$$a_1\alpha_1+\cdots+a_n\alpha_n, a_i\in F.$$

因为 a_i 只能取 p 个值，所以象上面形状的元互异的只有 p^n 个，因此 K 的元数 $q=p^n$．

于是我们得到

定理 1 假如 K 是元数为 q 的有穷体，它的质域是 F，那么它的特征数 $p\neq 0$，并且 $q=p^n$，这里 $n=(K:F)$．

我们知道，元数是有穷的群以及元数是有穷的环都不一定是交换的．譬如对称群 S_n 就不是交换群．假如 $R=Z-(p)$，p 是质数，那么全矩阵环 R_n 也不是交换环，但是元数是有穷的体却不是这样．任意有穷体都是域，这结论是 1905 年魏特邦(J. H. M. Wedderburn，1882～1948)提出的，是魏特邦著名定理之一．因为证明比较麻烦，我们把证明放在这节后面，在这里我们先承认这个事实，因此下面的有穷体都假定是域．于是有穷体又叫有穷域，有时我们又叫做伽罗瓦域，下面是有穷域的基本性质．

假定有穷域 K 的元数是 q，那么它的乘群的元数就是 $q-1$，于是 K 中任意非零元 α 的阶数是 $q-1$ 的因数，因此

$$\alpha^{q-1}=e, \alpha\neq 0,$$

所以

$$\alpha^q=\alpha.$$

显然 $\alpha=0$ 也是这多项式的零点，这就是说，在元数是 q 的有穷域中，任意元的 q 次幂仍然是它自身．于是 K 中元都是 $F[x]$ 中多项式 $f(x)=x^q-x$ 的零点，因此 K 是多项式 $f(x)$ 的所有零点组成的域，所以 K 是 $f(x)$ 的分裂域，因而 K 也是 F 的正规域．根据 §5.5 定理 3，我们又有

定理 2 元数相等的有穷域是同构的．

我们知道，有穷域的元数是质数的乘幂，反过来，假如 p 是任

意质数，用它的任意正整数幂 p^n 做元数的有穷域是否存在?

由§5.2，元数是 p 的质域 F 是存在的．从 F 作 $F[x]$ 中多项式 $f(x)=x^{p^n}-x$ 的分裂域 K．假如 α,β 是 $f(x)$ 在 K 的零点，即 $\alpha^{p^n}=\alpha,\beta^{p^n}=\beta$，那么

$$(\alpha-\beta)^{p^n}=\alpha^{p^n}-\beta^{p^n}=\alpha-\beta,$$

并且当 $\beta\neq 0$ 时，

$$\left(\frac{\alpha}{\beta}\right)^{p^n}=\frac{\alpha^{p^n}}{\beta^{p^n}}=\frac{\alpha}{\beta}.$$

这就是说，在 K 中，$f(x)$ 的任意两个零点的差及商仍然是它的零点，因此 K 中 $f(x)$ 的所有零点成为域；再因为

$$f'(x)=p^nx^{p^n-1}-e=-e,$$

因此 $f(x)$ 没有重零点，也就是说，$f(x)$ 的 p^n 个零点是互异的．所以 K 是元数为 p^n 的域，于是我们有

定理3 对于任意质数 p 的乘幂 p^n，除同构的外，只有唯一个元数是 p^n 的有穷域，也就是伽罗瓦域．

因为一个伽罗瓦域由它的元数 p^n 唯一决定，元数是 p^n 这类型的伽罗瓦域我们用 $GF(p^n)$ 来表示．下面我们来讨论它的子域．

假如 K 是 $GF(p^n)$ 的子域，那么 K 也是伽罗瓦域．因为 K 的特征数与 $GF(p^n)$ 的特征数相同，所以 K 的特征数也是 p，因此 K 是伽罗瓦域 $GF(p^m)$．这时因为 $m=(K:F)$，所以 m 是 n 的因数，这就是说，$GF(p^n)$ 的子域只有象 $GF(p^m)$ 这样形状的，其中 m 是 n 的因数．但是对于 n 的任意因数 m，$GF(p^m)$ 也是 $GF(p^n)$ 的子域．下面的证明与§2.2定理5中有穷群的情况类似．

定理4 假设 m 是 n 的任意因数，那么 $GF(p^n)$ 中只有唯一个 $GF(p^m)$ 型的子域．

证明 因为 m 是 n 的因数，所以

$$p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\cdots+p^m+1),$$

于是 $x^{p^m-1}-1$ 是 $x^{p^n-1}-1$ 的因式，因此 $x^{p^m}-x$ 是 $x^{p^n}-x$ 的因式，但 $x^{p^n}-x$ 在 $GF(p^n)$ 中完全分裂，所以 $x^{p^m}-x$ 在 $GF(p^n)$ 中也完全分裂，于是 $GF(p^n)$ 中包含 $x^{p^m}-x$ 的 p^m 个零点，由这 p^m 个零点组成的子域就是伽罗瓦域 $GF(p^m)$. 再因为 $x^{p^m}-x$ 在 $GF(p^n)$ 中的分裂域只有唯一个，因此 $GF(p^n)$ 中只有唯一个 $GF(p^m)$ 型子域，所以定理得证．

于是，我们得知伽罗瓦域 $GF(p^n)$ 中子域的个数等于 n 中互异正因数的个数．有穷循环群也是这样，n 元循环群的子群个数等于 n 中互异正因数的个数．在群中，循环群的构造以及它的子群的个数是已经知道了的，与这类似，在体中，对于伽罗瓦域，这两个问题也算是解决了的．

由 § 5.7 定理 3，我们得知伽罗瓦域 $GF(p^n)$ 是它的质域 F 的单扩张域，即 $GF(p^n)=F(\alpha)$，又因为 $x^{p^n}-x$ 没有重零点，所以 α 是 F 的可离元，于是 $GF(p^n)$ 是 F 的可离域．但 $GF(p^n)$ 的任意子体 K 都包含 F，所以 $GF(p^n)$ 又是 K 的可离域．

下面，我们来讨论 $GF(p^n)$ 的乘群．因为乘群中元是多项式 $x^{p^n-1}-e$ 的零点．我们从一般情况开始．

定义 假设 e 是域 F 的单位元，h 是正整数，那么

$$f(x)=x^h-e$$

在 F 的扩张体中的零点，叫做 F 的 h 次单位根，有时简单地叫做 h 次单位根．

当 h 不能用 F 的特征数 p 整除即 h 与 p 互质或 $p=0$ 时，因为 $f'(x)=hx^{h-1}$，显然 $f(x)$ 没有重零点，因此在 $f(x)$ 的分裂域中，h 次单位根恰有 h 个．

阶数是 h 的 h 次单位根，叫做 h 次本原单位根．我们知道，假如 α 是 F 的 h 次本原单位根，那么 α^m 是 h 次本原单位根的必要充分条件是 m 与 h 互质，即 $(m,h)=1$. 因此，F 的 h 次本原单位根的个数等于 $\varphi(h)$. 假如 h 能用 $p(\neq 0)$ 整除，$h=qp^k$，$(q,p)=1$. 因为 $x^h-1=(x^q-1)^{p^k}$，所以这时 F 没有阶数是 h 的单位根，也就是

说没有 h 次本原单位根．因此，如果 F 含有 h 次本原单位根，那么 h 与 p 就互质．

在§2.2中，我们得知复数域中 n 次单位根成为 n 元循环群，这性质在一般域中也成立．

定理5 假定 h 是不能用域 F 的特征数整除的正整数，那么在 F 的适当扩张域中，F 的所有 h 次单位根组成元数是 h 的循环群．

证明 假设 $\alpha^h=e,\beta^h=e$，那么

$$(\alpha\beta^{-1})^h=\alpha^h\beta^{-h}=e,$$

因此 x^h-e 的所有零点对乘法形成为群 G，这时 G 的元数显然是 h，下面证明 G 是循环群．

我们把 h 分解为质数幂的乘积，即 $h=\prod\limits_{i=1}^{m}p_i^{r_i}$．假如在 G 中我们能够找到阶数是 $p_i^{r_i}$ 的元 a_i，由§2.2习题5，$a=\prod\limits_{i=1}^{m}a_i$ 就是 G 中阶数是 h 的元，因此 $G=(a)$，于是 G 就是循环群．

由§3.10，我们知道 n 次多项式在域中零点不能多于 n 个，因此多项式

$$x^{\frac{h}{p_i}}-e,$$

在 G 中最多只有 $\frac{h}{p_i}$ 个零点，于是 G 中最少有一个使 $b_i^{\frac{h}{p_i}}\neq e$ 的元 b_i，我们把 $b_i^{(h/p_i^{r_i})}$ 写成 a_i，即 $a_i=b_i^{(h/p_i^{r_i})}$．因为 $a_i^{p_i^{r_i}}=b_i^h=e$，所以由§2.2习题3，a_i 的阶数是 $p_i^{r_i}$ 的因数，但

$$a_i^{p_i^{r_i-1}}=b_i^{\frac{h}{p_i}}\neq e,$$

因此 $a_i^{p_i^{s_i}}\neq e,s_i<r_i$．于是 a_i 的阶数是 $p_i^{r_i}$，所以定理得证．

在上定理中，如果 h 能够用 F 的特征数 p 整除，即 $h=qp^s$，$(q,p)=1$，因为 $x^h-e=(x^q-e)^{p^s}$，因此 F 的 h 次单位根是 q 次单位根，所以这时 F 的所有 h 次单位根只有 q 个，于是上定理中的 G 是 q 元循环群．

由上定理的证明，我们容易得知 G 所以能够成为循环群是因为其中满足 $x^{\frac{h}{p_i}}=e$ 的元不多于 $\frac{h}{p_i}$ 个．反过来，假如 $G=(a)$ 是 n 元循环群，m 是 n 的任意因数，显然其中满足 $x^m=e$ 的元只有 $a^{\frac{n}{m}i}$，$i=0,1,\cdots,m-1$. 因此 n 元交换群 G 是循环群的必要充分条件是：对于 n 的任意因数 m，G 中满足 $x^m=e$ 的元不多于 m 个．在 §2.2 中我们给出了循环群的一个必要充分条件，这里我们又得到另一个必要充分条件[9].

现在我们引用上面的结论，推得下面伽罗瓦域乘群的一个重要性质．

因为 $GF(p^n)$ 的乘群 G 中元都是多项式 $x^{p^n-1}-e$ 的零点，由定理 5，我们得知 G 是循环群，即

定理 6 有穷域的乘群是循环群．

这是有穷域的一个重要性质．因为 n 元群中 n 个元是互异的 n 次单位根，由 §3.10 定理 3 及上面定理 5，我们又可以把这性质推广到任意域，也就是说，任意域的乘群的有穷子群都是循环群．此外，对一般非交换体，我们还有

定理 7 假定 K 是特征数为 $p(\neq 0)$ 的体，G 是它的乘群的有穷子群，那么 G 是循环群．

证明 假定 F 是 K 的质域，

$$L=\{\sum a_i g_i \mid a_i\in F, g_i\in G\}$$

显然，L 对加法、乘法都是闭合的，因此 L 成环，再因为 F，G 都是有穷集，所以 L 就是有穷环，于是，L 是元数为有穷的无零因子环，因此 L 成体，即 L 是有穷域．所以 L 的乘群是循环群，显然 G 是乘群的子群，因为循环群的子群是循环群，所以 G 是循环群，证毕．

对于一般特征数是 0 的体，这性质不一定成立[10]. 譬如四元数体的有穷子群 $\{\pm e, \pm i, \pm j, \pm k\}$ 就不是循环群．

下面我们来证明魏特邦定理．先介绍分圆多项式，以备引

用.

假定$\xi_1,\cdots,\xi_{\varphi(n)}$是$n$次复数本原单位根,那么

$$\Phi_n(x)=\prod_{i=1}^{\varphi(n)}(x-\xi_i)$$

叫做n次**分圆多项式**. 由计算容易得知,

$$\Phi_1(x)=x-1,\qquad \Phi_2(x)=x+1,$$
$$\Phi_3(x)=x^2+x+1,\Phi_4(x)=x^2+1.$$

再我们有

$$x^n-1=\prod_{d|n}\Phi_d(x),$$

式中d取n的所有正因数,这是因为任意n次单位根是某个d次本原单位根. 反过来,任意d次本原单位根都是n次单位根. 又分圆多项式$\Phi_n(x)$的系数都是整数,这是因为,$\Phi_1(x)=x-1$的系数是整数,如果对于$0<d<n$,$\Phi_d(x)$的系数是整数,由§3.5,我们得知用首项系数是1的整系数多项式$\prod_{d\neq n}\Phi_d(x)$除整系数多项式x^n-1得到的商$\Phi_n(x)$仍然是整系数多项式.

因为$d|n$,所以$x^n-1=\Phi_n(x)(x^d-1)g(x)$,即

$$\Phi_n(x)\left|\frac{x^n-1}{x^d-1}\right..$$

又假定q是不小于2的有理数,如果$n=1$,那么

$$|\Phi_n(q)|=q-1;$$

如果$n>1$,我们命ξ是n次复数本原单位根,显然

$$|q-\xi|>|q|-|\xi|=q-1\geqslant 1$$

因此

$$|\Phi_n(q)|=\prod_{i=1}^{\varphi(n)}|q-\xi_i|>q-1.$$

最后,我们引用上面的性质来证明**魏特邦定理**. 这定理是1905年魏特邦首先证明的,此后再来证明的颇不乏人,下面叙述的是1931年威特(E. Witt,1911~)提出的一个初等证明[11].

定理8(Wedderburn) 有穷体是域.

假设K是有穷体,F是它的中心,$(K:F)=n$,α是K中任意

非零的元，显然，K 中所有与 α 能够交换的元集合

$$L=\{x \mid x \in K, x\alpha=\alpha x\}$$

形成一个体，并且 $K \supseteq L \supseteq F$. 假定 F 的元数是 q，那么 K 及 L 的元数分别是 q^n、q^d，这里 $d=(L:F)$，$d \mid n$. 如果我们能够证明 $d=n$，那么 $L=K$，因此 $\alpha \in F$，于是 K 就是域了.

我们用反证法来证明. 假定 $d<n$，那么 $n>1$，我们把 K 的乘群分为若干个共轭类. 我们知道，如果 $\alpha \in F$，那么 α 自身成为一共轭类，如果 $\alpha \overline{\in} F$，由§2.4 得知 α 所在的共轭类的元数是 $\frac{q^n-1}{q^d-1}$，这里 $d \neq n$，于是

$$q^n-1=q-1+\sum_{d \mid n} \frac{q^n-1}{q^d-1}, d \neq n.$$

因为 $\Phi_n(x)$ 是 x^n-1 的因式，并且当 $d<n$ 时，$\Phi_n(x)$ 不是 x^d-1 的因式，所以 q^n-1 及 $\frac{q^n-1}{q^d-1}(d<n)$ 都能够用 $\Phi_n(q)$ 整除，因此 $q-1$ 也能够用 $\Phi_n(q)$ 整除，这与 $q \geqslant 2, n>1$ 时，$|\Phi_n(q)|>q-1$ 的性质不合，因此 $n=d$，所以定理得证.

1945 年贾柯勃逊(N. Jacobson，1910～)有这样一个定理：假定对于环 R 中任意元 a，存在与 a 有关的整数 $n(a)>1$，使 $a^{n(a)}=a$，那么 R 就是交换环[12]. 这定理可以说是上面魏特邦定理的推广. 1954 年赫尔司顿(I. N. Herstain，1923～)有一个初等证明. 1971 年温沙(J. W. Wansley)另有一个初等证明[13]. 上面的贾柯勃逊定理只是环为交换环的一个充分条件而不是必要条件，并且是一个很苛刻的条件，就是最普通的整数环也不能适合. 1957 年赫尔司顿给出一个必要充分条件，1959 年富永久雄(1927～)对这有所推广，1971 年贝尔(H. E. Bell)又有推广[14]，读者如欲知其详，请取原始资料参考.

习 题 5.8

1. 试证费马(P. D. Fermat，1601～1665)定理：

$$a^{p-1}\equiv 1(p),$$

这里 p 是质数,a 是任意与 p 互质的整数.

2. 假如 F 是特征数为 p 的质域,α 是 $F[x]$中 m 次既约多项式 $f(x)$在 $GF(p^m)$中的零点,试证 $\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^m}=\alpha$ 是 $f(x)$的全部零点.

3. 试证伽罗瓦域是完全域.

4. 假如 K 是特征数为 p 的伽罗瓦域,a 是其中任意元,试证在 K 中,a 的 p 次根只有一个 $a^{\frac{1}{p}}$.

5. 假定 K 是有穷域,特征数$\neq 2$,α,β 是 K 中两个非零元,那么在 K 中有元 a,b,使得 $1+\alpha a^2+\beta b^2=0$.

6. 试证分圆多项式 $\Phi_n(x)$是正规式.

7. 试求作 $GF(3^2)$的加法及乘法表.

§5.9　超越扩张体

我们知道,域 F 的扩张体如果不是 F 的代数体,就叫做 F 的超越体.前面五节讨论的主要是代数体,这节我们来讨论超越体.我们这样来讨论,把 F 的超越体看成是某 $F(M)$的代数体,这里集合 M 中元当然是 F 的超越元,因此,使用的方法及得到的结果都与§5.4中讨论代数体的类似.在讨论代数体时,体的次数及基底是两个基本概念,现在我们需要与它们类似的概念,因此首先我们把线性相关、线性无关的概念来推广.

假定 u 是 F 的扩张域 K 中元,M 是 K 的有穷子集,如果 u 是域 $F(M)$的代数元,那么 u 叫做关于 F 与 M **代数相关**,否则就叫做关于 F 与 M **代数无关**.

根据定义,我们容易得知,u 关于 F 与 $M=\{u_1,\cdots,u_m\}$代数相关的必要充分条件是:u 是多项式

$$\sum_{i=0}^{n} f_i(u_1,\cdots,u_m)x^i,\ f_n(u_1,\cdots,u_m)\neq 0$$

的零点,这里 $f_i(x_1,\cdots,x_m)$是 $F[x_1,\cdots,x_m]$中元.

假如 M 中有一元关于 F 与 M 中其余元代数相关,那么 M 叫

做关于 F 代数相关，否则就叫做关于 F 代数无关．于是 F 的代数元关于 F 代数相关；F 的超越元关于 F 代数无关．

显然，假如 M 关于 F 代数无关，那么 M 的任意子集关于 F 代数无关；假如 M 关于 F 代数相关，那么任意包含 M 的有穷集关于 F 代数相关．再假如 u 关于 F 与 M 线性相关，那么 u 关于 F 与 M 代数相关；假如 M 关于 F 代数无关，那么 M 关于 F 线性无关．

下面是代数相关的基本性质，这些性质也是线性相关具备的．

1．假定 $u\in M$，那么 u 关于 F 与 M 代数相关．

这是因为 u 在 $F(M)$ 中，所以 u 是关于 $F(M)$ 的代数元，因此 u 关于 F 与 M 代数相关．

2．假定关于 F，v 与 $M=\{u_1,\cdots,u_m\}$ 代数相关，但与 $\{u_1,\cdots,u_{m-1}\}$ 代数无关，那么 u_m 关于 F 与 $\{u_1,\cdots,u_{m-1},v\}$ 代数相关．

这是因为 v 关于 F 与 M 代数相关，所以我们有

$$\sum_{i=0}^{r}f_i(u_1,\cdots,u_m)v^i=0,\ f_r(u_1,\cdots,u_m)\neq 0.$$

我们把上式左边多项式写成 u_m 的多项式 $\sum_{i=0}^{s}g_i(u_1,\cdots,u_{m-1},v)u_m^i$ 就得到

$$\sum_{i=0}^{s}g_i(u_1,\cdots,u_{m-1},v)u_m^i=0.$$

因为 v 关于 F 与 $\{u_1,\cdots,u_{m-1}\}$ 代数无关，所以，对于任意 g_i，不是 $g_i(u_1,\cdots,u_{m-1},v)\neq 0$，便是 $g_i(u_1,\cdots,u_{m-1},v)$ 关于 v 恒等于零，即 $g_i(u_1,\cdots,u_{m-1},x)$ 的系数都为零．假如所有的 $g_i(u_1,\cdots,u_{m-1},x)\equiv 0$，那么

$$\sum_{i=1}^{r}f_i(u_1,\cdots,u_m)x^i\equiv 0,$$

因此 $f_r(u_1,\cdots,u_m)=0$，这与假设不合．于是所有的 $g_i(u_1,\cdots,u_{m-1},v)$ 不能完全都是零，所以 u_m 关于 F 与 $\{u_1,\cdots,u_{m-1},v\}$ 代数相关．

特别，假如关于 F，α 是超越元，并且与 β 代数相关，那么 β 关于 F 与 α 代数相关．

3. 假定关于 F，v 与 M 代数相关，并且 M 中任意元与 N 代数相关，那么 v 关于 F 与 N 代数相关．

这是因为 v 是 $F(M)$ 的代数元时，它当然也是 $F(M,N)$ 的代数元，因此 $F(M,N)(v)$ 是 $F(M,N)$ 的代数域．然而 $F(M,N)$ 是 $F(N)$ 的代数域，由§5.4定理2，$F(M,N)(v)$ 是 $F(N)$ 的代数域，所以 v 是 $F(N)$ 的代数元，因此 v 关于 F 与 N 代数相关．

4. 假定关于 F，M 代数无关，但 $M\cup u$ 代数相关，那么 u 与 M 代数相关．

这是因为关于 F，$M\cup u$ 代数相关，所以 $M\cup u$ 中某元 v 与 $M\cup u-v$ 代数相关．如果 $u=v$，那么 u 与 M 代数相关；如果 $u\neq v$，那么 $v\in M$，因为 M 代数无关，所以 v 与 $M-v$ 代数无关，因此由2，u 与 M 代数相关．

5. 假定关于 F，有穷集 M 代数无关，并且 M 中任意元与有穷集 N 代数相关，那么 M 的元数不大于 N 的元数，即 $|M|\leqslant|N|$．

这是因为关于 F，在 $M\cup N$ 中显然有代数无关的 $|M|$ 元子集，因为 M 就是这样的子集．在所有这些 $|M|$ 元子集中，假设 M' 是含 N 中元最多的一个子集，并且假定这最多元数是 $n(\geqslant 0)$．假如 $n<|M|$，我们命 u 是 M' 中而不是 N 中元，v 是 N 中任意元，如果 $v\in M'-u$，那么 v 与 $M'-u$ 代数相关；如果 $v\bar{\in} M'-u$，因为 $|M|$ 元子集 $(M'-u)\cup v$ 含 N 中 $n+1$ 个元，根据 n 是最大的假设，我们得知 $(M'-u)\cup v$ 代数相关，但 $M'-u$ 代数无关，由4我们也得到 v 与 $M'-u$ 代数相关，这就是说，无论如何 N 中任意元与 $M'-u$ 代数相关．因为 $u\in M$，根据假设 u 与 N 代数相关，于是由3，u 与 $M'-u$ 代数相关，这与 M' 代数无关的假设不合，因此 $n=|M|$，所以 $|N|\leqslant|M|$．于是我们容易得知 M 中关于 F 不同的最大无关组的元数是相等的．

上面的 M 都假定是有穷集，假如 M 是无穷集，如果 u 关于 F

与 M 的任意有穷子集代数无关，那么 u 就叫做关于 F 与 M 代数无关；否则，也就是说，u 关于 F 与 M 的某有穷子集代数相关，那么 u 就叫做关于 F 与 M 代数相关．再如果 M 中任意有穷个元关于 F 都是代数无关，那么 M 就叫做关于 F 代数无关；否则，也就是说，M 中某有穷个元关于 F 代数相关，那么 M 就叫做关于 F 代数相关．这与向量空间中无穷个元线性无关，线性相关的概念完全一致．

下面是代数无关的一个基本性质．

我们知道，一个元关于 F 代数无关的必要充分条件是它不适合 $F[x]$中任意非零的多项式．一般这性质也是成立的．

定理 1 m 元集合 $M=\{u_1,\cdots,u_m\}$关于 F 代数无关的必要充分条件是对于 $F[x_1,\cdots,x_m]$中任意元 $f(x_1,\cdots,x_m)$，如果 $f(u_1,\cdots,u_m)=0$，那么

$$f(x_1,\cdots,x_m)=0,$$

即 $f(x_1,\cdots,x_m)$的系数都是零．

证明 假如当 $f(u_1,\cdots,u_m)=0$ 时，$f(x_1,\cdots,x_m)=0$，显然 M 中没有一元关于 F 与其余元代数相关，所以 M 关于 F 代数无关，因此条件的充分性成立．

再假如 M 关于 F 代数无关，并且 $f(u_1,\cdots,u_m)=0$，命

$$f(x_1,\cdots,x_m)=\sum_{i=0}^{n}f_i(x_1,\cdots,x_{m-1})x_m^i,$$

就元 u 的个数用归纳法来证明 $f(x_1,\cdots,x_m)=0$. 当元数=1 时，f_i 是 F 中元，因为 u_1 关于 F 代数无关，所以 $f_i=0$，因此 $f(x_1)=0$，所以元数=1 时条件成立．假定元数$=m-1$ 时条件成立，因为 M 关于 F 代数无关，所以 $f_i(u_1,\cdots,u_{m-1})=0$，$i=0,\cdots,n$. 又因为 $u_1,\cdots,u_{m-1}$关于 F 代数无关，根据归纳法的假设，我们有 $f_i(x_1,\cdots,x_{m-1})=0$，于是 $f(x_1,\cdots,x_m)=0$. 于是条件的必要性($\forall\, m\in N$)成立．所以定理得证．

于是 m 个元 $u_1,\cdots,u_m$，如果是代数相关，那么它们之间有代

数方程相联系;如果无关,那么它们之间不存在任何代数方程的联系.

假定$\{u_1,\cdots,u_n\}$关于F代数无关,$x_1,\cdots,x_n$是F的未定元,显然

$$f(x_1,\cdots,x_n)\to f(u_1,\cdots,u_n)$$

是多项式环$F[x_1,\cdots,x_n]$,$F[u_1,\cdots,u_n]$的同构,于是它们的分式域$F(x_1,\cdots,x_n)$,$F(u_1,\cdots,u_n)$也同构,也就是说

$$F(x_1,\cdots,x_n)\simeq F(u_1,\cdots,u_n).$$

因此代数无关的元我们可以看成未定元,它们之间可以不加区别.

上面,我们介绍了代数相关、代数无关的基本性质,现在我们来讨论超越扩张体.

定义 假定K是F的扩张域,那么K中关于F代数无关子集的最大元数,叫做K关于F的超越次数.假定$M=\{u_1,\cdots,u_m\}$是K中关于F代数无关的子集,如果K中任意元关于F与M代数相关,那么$u_1,\cdots,u_m$叫做K关于F的代数底.

因为F的代数域中任意元关于F代数相关,所以F的代数域关于F的超越次数是零,因此它没有关于F的代数底.反过来也成立,这就是说,F的扩张域是代数域的必要充分条件是它关于F的超越次数是零.

再在F的超越单扩张域$F(x)$中,x关于F代数无关,任意元$u=\dfrac{f(x)}{g(x)}$,因为$ug(x)-f(x)=0$,所以u与x关于F代数相关,因此,x就是$F(x)$关于F的代数底.再由5,用反证法得知$F(x)$中任意两元关于F代数相关.因此$F(x)$关于F的超越次数是1.若$\{x_1,\cdots,x_n\}$关于F代数无关,则F的超越体$F(x_1,\cdots,x_n)$关于F的超越次数是n,并且$x_1,\cdots,x_n$就是它关于F的代数底.

依定义K关于F的超越次数是K中关于F最大无关组的元数,由5这最大无关组就是K关于F的代数底.于是,我们有下

面与§4.1定理3类似的定理.

定理2 K 关于 F 的代数底的元数等于 K 关于 F 的超越次数.

于是同代数域一样,一般超越域的各个代数底的元数都相等,它们都等于体的超越次数.

我们知道在 F 的扩张体 K 中,除 F 中元外,如果没有 F 的代数元,那么 K 就叫做 F 的纯超越体. 添加 F 的超越元于 F 扩张的体当然是 F 的超越体,但它是否就是 F 的纯超越体?

我们先来考虑超越单扩张域 $F(x)$. 因为其中任意元 u 是系数为 F 中元的 x 的有理函数,假如命 $u=\dfrac{f(x)}{g(x)}$,这里 $f(x),g(x)$ 是 $F[x]$ 中互质的多项式,根据§3.9定理7,$f(x),g(x)$ 除 F 中非零元的因子外,由 u 唯一决定,因此它们的次数也是由 u 唯一决定,我们叫 $f(x),g(x)$ 的次数中较大的做 u 关于 F 的**超越次数**.

定理3 假定 u 是 F 的超越单扩张域 $F(x)$ 中关于 F 超越次数 $n>0$ 的元,那么 u 是 F 的超越元,并且 $F(x)$ 是 $F(u)$ 的 n 次代数域.

证明 假定 $u=\dfrac{f(x)}{g(x)}$,这里 $f(x),g(x)$ 互质,因为 $ug(x)-f(x)=0$,所以 x 是 $F(u)[y]$ 中多项式 $h(y)=ug(y)-f(y)$ 的零点. 但 $f(y),g(y)$ 的次数都 $\leqslant n$,并且至少有一是 n,而 u 又不是 F 中元,因此 $h(y)$ 的次数是 n. 假如我们还能够证明 $h(y)$ 是既约的,那么 x 是 $F(u)$ 的 n 次代数元. 因此,$F(x)$ 是 $F(u)$ 的 n 次代数域. 显然,u 是 F 的超越元,因为不如此,x 就是 F 的代数元了.

假如 $h(y)$ 在 $F(u)[y]$ 中是可约的,$h(y)=h_1(y)h_2(y)$,设

$$h_1(y)=\frac{a}{b}h_1(u,y),h_2(y)=\frac{c}{d}h_2(u,y),$$

这里 $h_1(u,y),h_2(u,y)\in F[u,y]$. 于是

$$h(y)=h(u,y)=\frac{ac}{bd}h_1(u,y)h_2(u,y)$$

因为 $bd|ac$,所以在 $F[u,y]$ 中,我们有

$$h(u,y)=k_1(u,y)k_2(u,y)$$

因为 $h(y)$ 是 u 的 1 次式，所以 $k_1(u,y),k_2(u,y)$ 中有一个只含 y 而不含 u. 设 $k_2(u,y)=k_2(y)$，于是 $k_2(y)\mid h(u,y)$. 因此

$$k_2(y)\mid f(y);k_2(y)\mid g(y),$$

即 $k_2(y)$ 是 $f(y),g(y)$ 的公因式，这与 $f(x),g(x)$ 互质的假设不合，因此 $h(y)$ 在 $F(u)[y]$ 中是既约的. 这就是说，x 是 $F(u)$ 的 n 次代数元，于是定理成立.

特别当 $n=1$ 时，显然 $F(x)=F(u)$，这就是说，$F(x)$ 中任意关于 F 超越次数是 1 的元都是 $F(x)$ 关于 F 的本原元. 显然，$F(x)$ 关于 F 的本原元也只能是这样超越次数是 1 的元，因此我们得知 u 是 $F(x)$ 关于 F 的本原元的必要充分条件是

$$u=\frac{ax+b}{cx+d},ad-bc\neq 0.$$

因为在 $F(x)$ 中除 F 中元外，任意元关于 F 的次数>零，由定理 3，它是 F 的超越元，因此 $F(x)$ 是 F 的纯超越扩张体. 一般有

定理 4 假定 $\{x_1,\cdots,x_n\}$ 关于域 F 代数无关，那么 F 的超越域 $K=F(x_1,\cdots,x_n)$ 是 F 的纯超越体.

证明 我们用归纳法来证明. 当 $n=1$ 时，定理成立. 假定 $n-1$ 时定理成立，我们命 α 是 K 中关于 F 的任意代数元，因此 α 也是 $F(x_1,\cdots,x_{n-1})$ 的代数元，并且 K 是 $F(x_1,\cdots,x_{n-1})$ 的纯超越体，所以 $\alpha\in F(x_1,\cdots,x_{n-1})$. 再由归纳法的假设，我们就有 $\alpha\in F$，这就是说，K 中 F 的任意代数元是 F 中元，因此 K 是 F 的纯超越体，所以定理成立.

假定 K 是 F 的扩张域，$u_1,\cdots,u_n$ 是它关于 F 的代数底，那么 K 中任意元是 $L=F(u_1,\cdots,u_n)$ 的代数元，因此 L 是 K 中次数最大的 F 超越域，并且 L 又是 F 的纯超越体，于是我们得知，K 可以先自 F 纯超越扩张，然后再代数扩张而成. 这与 §5.4 中任意扩张域可以先代数扩张再纯超越扩张而成的步骤恰相反.

最后我们介绍鲁洛斯(J. Lueroth，1844～1910)定理，它在几

何上还有重要的应用.

定理 5 假定 L 是 F 的超越单扩张域 $K=F(x)$ 与 F 的中间体，并且异于 F，即 $K\supseteq L\supset F$，那么 L 是 F 的超越单扩张体.

证明 假定 u 是在 L 中而不是 F 中元，因为 x 是 $F(u)$ 的代数元，所以也是 L 的代数元，我们命

$$g(y)=y^n+a_1y^{n-1}+\cdots+a_n, a_i\in L,$$

是 $L[y]$ 中 x 适合的既约多项式. 因为 a_i 是 x 的有理函数，所以我们有 $k(x)\in F[x]$，使 $f(x,y)=k(x)g(y)$ 是 $F[x,y]$ 中元，并且 $f(x,y)$ 写成 y 的多项式时，它的系数的最大公因式是 1，就是说，$f(x,y)$ 是 $F[x]$ 的本原多项式(§3.9)，$f(x,y)$ 对于 x 的次数假定是 m，对于 y 的次数当然是 n.

因为 $(L(x):L)=n$，而 $L(x)=F(x)$，所以 $(F(x):L)=n$. 假如 L 中有关于 F 超越次数是 n 的元 a，那么由定理 3,

$$(F(x):F(a))=n,$$

但 $L\supseteq F(a)$，所以 $L=F(a)$——L 是 F 的超越单扩张域. 证毕.

因为 x 是 F 的超越元，所以 $g(y)$ 的系数 a_i 不能完全都是 F 中元，我们假定 a_j 不在 F 中，并且把 a_j 写成

$$a=a_j=\frac{p(x)}{q(x)}=\frac{l(x)}{k(x)},$$

这里 $p(x)$ 与 $q(x)$ 互质. 因为 $f(x,y)$ 对于 x 的次数是 m，所以 $l(x)$，$k(x)$ 的次数都 $\leqslant m$，因此 $p(x)$，$q(x)$ 的次数也都 $\leqslant m$.

再因为 $p(y)-aq(y)$ 是 $L[y]$ 中 x 适合的多项式，所以它能用 $g(y)$ 整除，于是我们有

$$p(y)-\frac{p(x)}{q(x)}q(y)=r(x)v(y)g(y)$$

$$=\frac{r(x)}{s(x)k(x)}t(x,y)f(x,y),$$

因此

$$q(x)p(y)-p(x)q(y)=\frac{q(x)r(x)}{s(x)k(x)}t(x,y)f(x,y),$$

这里$t(x,y)$同$f(x,y)$一样是$F[x,y]$中本原多项式，由§3.9习题6，我们得知两个本原多项式$t(x,y)$，$f(x,y)$的乘积$t(x,y)\cdot f(x,y)$仍是$F[x,y]$的本原多项式，所以$s(x)k(x)|q(x)r(x)$. 因此

$$q(x)p(y)-p(x)q(y)=h(x,y)f(x,y),$$
$$h(x,y)\in F[x,y],$$

这时左边对于x的次数不大于m，而右边$f(x,y)$对于x的次数是m，因此，左边对于x的次数也是m，所以$h(x,y)$不含x，即右边没有是$F[x]$中多项式的因式. 假如$h(x,y)$含y，因为左边是x,y的对称式，所以x的多项式$h(y,x)$是它的因式，这与上面矛盾. 因此$h(x,y)$又不含y，于是$h(x,y)=h\in F$，即

$$q(x)p(y)-p(x)q(y)=hf(x,y).$$

由x,y的对称性，我们得知$f(x,y)$对于y的次数是m，所以$m=n$. 因此$p(x)$，$q(x)$中至少有一是x的n次多项式. 于是α的超越次数是n，所以定理得证.

由上面的证明，我们又知道$g(y)$中不是F中元的系数都是关于E的本原元.

这结论在超越次数是2时只有在一定的条件下才成立. 在超越次数大于2时即使F是代数闭体也不能成立，也就是说鲁洛斯定理不能推广.

把这定理与§5.7定理4合并，我们就得到：

定理6 域F的任意单扩张域与F的中间体是F的单扩张域.

习 题 5.9

1. 假定K关于L的超越次数是m，L关于F的超越次数是n，试证K关于F的超越次数是$m+n$.

2. 假定$\{u,v\}$关于F代数无关，试证$\{u^3+v^2,v^2+u\}$关于F代数无关，并且

$$(F(u,v):F(u^3+v^2,v^2+u))=6.$$

3. 怎样的对应是$F(x)$不使F中任意元变动的自同构?

4. 试用本节所述方法证明 § 5.3 定理 3.

参 考 文 献

[1] E. Steinitz, Algebraische Theorie der Körper, Herausges von R. Baer und H. Hasse, Berlin(1930).

[2] E. Snapper, Completely primary rings I, Ann. of Math., 52(1950), 666～673; II, Ann of Math., 53(1951), 125～142; III, Ann. of Math., 53(1951)207～234; IV. Ann. of Math., 55(1953), 46～64.

[3] A. A. Albert, Structure of algebras(1939)
P. M. Cohn, Skew field Construction(1979)
P. X. Draxl, Skew fields (1984)
John Dauns, A concrete approach to division rings.

[4] Slanozevie, Caslar, A sufficient and necessary condition for division rings, Bull. Soc. Math. Phys. Macédoine 12(1963), 25～29.
T. P. Kezlan, Rings without zero divisors, Amer. Math, Monthly, 74(1967), 1016～1017.

[5] R. W. Ball, A theorem On groups and the characteristic of an integral Domain, Amer. Math. Monthly 73(1966), 1113.

[6] O. Zariski and P. Samnal, Commutative Algebra, vol. 1(1958), 106～107.

[7] J. Sonn, H. Zassenhaus, On the theorem of the primitive elements, Amer. Math. Monthly 74(1967), 407～410.

[8] E. Artin, Galois Theory (1946), 64～65.
P. Wilker, über die Zwischerkörper einfacher Algebraisher Erweiterungen, Math. Ann., 124(1952), 289～290.

[9] J. H. E. Cohn, A condition for a finite groups to be cyclic, Proc. Amer. Math. Soc., 32(1972), 48.

[10] I. N. Herstain, Finite multiplicative subgroups in division rings, Pacific Jour. of Math., 3(1953), 121～126.

[11] H. Goheen, The Wedderburn Theorem, Can. Jour. of Math., 7(1955), 60～62.
E. Witt. über die Kommutativitätendlichen Schiefkörper, Abh. Math. Sem. Univ., Hamburg, 8(1931), 413.

I. N. Herstain, Wedderburn's theorem and a Theorem of Jacobson, Amer. Math. Monthly, 68(1961), 249～251.

P. W. Hendeuson, A short proof of Wedderburn's theorem, Amer. Math. Monthly, 72(1965), 385～386.

[12] N. Jacobson, Structure theory for algebraic algebras of bounded degree, Ann. of Math., 46(1945), 695～707.

Huzurbazar, M. S., Sivarama Hrishnan, K., Jacobson's theorem On Commutativity of rings, Aligarh Bull. Math. 1(1971), 9～12.

[13] N. N. Herstain, An elementary proof of a theorem of Jacobson, Duke Math. Jour., 21(1954), 45～48.

——, On a result of Faith, Can. Math. Bull. 18(1975), no. 4, 609.

J. Luh, On the Commutativity of J－rings, Canadian J. of Math. 10 (1967), 1289～1292.

Wausley, J. W., On a Condition for Commutativity of rings, J. London Math. Soc. (2)4(1971)331～332.

[14] I. N. Herstein, A condition for the commutativity of rings, Can. Jour. of Math., 9(1957), 583～586.

Tominaga, Hisao(富永久雄), A theorem on rings, Math. J. Okayama Univ., 9(1959). 9～12.

Bell, Howard E, On some Commutativity Theerem of Herstein, Aach Math. 24(1971), 34～38.

第6章

群　论

群的基本概念及基本性质在第二章已详细介绍，这章主要是讨论群的构造．

§6.1 算　子

由§4.1我们知道向量空间是一个加群，它除了有它自身的加法结合法外，还有与另一集合的乘法结合法；模也是如此．现在我们根据这把§2.1中群的概念来推广．首先引入这个概念的是克努尔(W. Krull，1889～)及诺特尔(E. Noether，1882～1935)．

定义1　假定G是群，M是集合，如果对于M中任意元λ，G中任意元a，b有

$$\lambda a \in G, \lambda(ab) = \lambda a \cdot \lambda b,$$

那么λ叫做G的(左)算子，M叫做G的(左)算子集，G叫做带(左)算集M的群，有时又叫做M-(左)群，或简单地叫做带算群．

譬如，任意整数n是交换群的算子．再假如R是环，其中任意元是R看成加群时的一个算子．

我们容易知道群G的自同态是G的算子，因此任意群都有算子集，也就是说都可以看成带算群．如在第二章那样不考虑算子集的群，我们可以说它的算子集是空集或者就是一个恒等同态．

假如M是群G的算子集，λ是M中任意元，显然$a \to \lambda a$是G的自同态，因此M中任意元可以看成为G的自同态，也就是说M是G的自同态集合．但要注意的是，算子与同态是有区别的，两

个不同的算子可能是同一个同态．譬如整数集 Z 是加群 Z_6 的算子集，但 $3\bar{a}=9\bar{a}$．即 3、9 二数虽不相等，但它们作为同态是一致的．根据同态的性质，我们得

$$\lambda e=e, \lambda a^{-1}=(\lambda a)^{-1}, \lambda a^n=(\lambda a)^n.$$

假如加群 G 的算子集是环 R，那么对于 R 中任意两元 u,v，我们要求

$$(u+v)a=ua+va, (uv)a=u(va), a\in G.$$

因此
$$(u-v)a=ua-va, 0a=0.$$

如果 R 有单位元 e，我们还要求

$$ea=a,$$

也就是说，R 的单位元是 G 的**单位算子**．于是整数环 Z 是交换群的算子集．一个环是以自身做带算集的加群．第四章讨论的 F 空间，F 的代数以及 R 模都是带算加群．

假如 G 是带算集 M 的群，它的子群不一定也是带算集 M 的群．如果 G 的子群 H 是带算集 M 的群，也就是说，对于 M 中的任意元 λ，H 中任意元 h，

$$\lambda h\in H,$$

那么 H 叫做 G 的**带算子群**．带算子群又是正规子群时，叫做**带算正规子群**．

群 G 的算子集假如是空集或者只是恒等同态，那么 G 的子群都是带算子群；假如是内同构群，那么它的带算子群都是正规子群；假如是自同构群，那么它的带算子群都是特征子群．假如环看成是用自身做左算子集的加群，那么它的带算子群就是它的左理想．

同§2.3中一样，假如带算交换群的元数是1或者是质数，那么它是单群．但要注意这性质的逆对一般的带算群并不成立，也就是说，一般带算交换单群的元数不一定是质数，譬如有理数域是以自身为带算集的单加群，但它的元数不是质数．

我们很容易证明，两个带算子群的交以及由它们生成的子群

都是带算子群.

在比较两个带算群,也就是在讨论两个带算群的同态、同构时,我们只考虑算子集是相同的情况.因此当我们比较群及它的商群时,首先要讨论,对于带算集 M 的群,它的怎样的商群也是带算集 M 的群,这时 M 与这商群的结合法又该怎样?

假如 H 是 G 的正规子群,λ 是 M 中任意元,如果 λ 又是商群 $\overline{G}=G/H$ 的算子,那么

$$\lambda H=H,$$

因此对于 H 中任意元 h,$\lambda h\in H$,所以 H 是 G 的带算正规子群.再因为

$$\lambda(ah)=\lambda a\cdot\lambda h\in\lambda a\cdot H, a\in G, h\in H,$$

所以
$$\lambda(aH)\subseteq\lambda a\cdot H.$$

于是我们就有

$$\lambda\overline{a}=\overline{\lambda a}. \tag{1}$$

这就是说,$\lambda\overline{a}$ 是 λa 所在的陪集 $\overline{\lambda a}$. 根据这关系,我们有

$$\lambda(\overline{a}\overline{b})=\lambda(\overline{ab})=\overline{\lambda(ab)}=\overline{\lambda a\cdot\lambda b}=\overline{\lambda a}\cdot\overline{\lambda b}=\lambda\overline{a}\cdot\lambda\overline{b}.$$

因此,假如 G 是带算集 M 的群,H 是它的带算正规子群,根据(1),那么 G/H 是带算集 M 的群.

显然,这时 G 到 $\overline{G}$ 上的同态 $a\to\overline{a}$ 具有性质

$$\lambda a\to\lambda\overline{a}.$$

引用上性质,我们可以把在第二章介绍的同构、同态等概念推广到带算群上来.

定义 2 假如 G,G' 都是算子集为 M 的带算群,σ 是 G 到 G' 上的同态,对于 M 中任意元 λ,当 $a\to a'=\sigma(a)$ 时,如果 $\lambda a\to\lambda a'$,也就是说

$$\sigma(\lambda a)=\lambda(\sigma(a)), a\in G,$$

那么 σ 叫做 G 到 G' 上的带算集 M 的同态,或简单地叫做带算同态,这时又叫 G,G' 是带算同态.带算同态映射是双射时,叫做带算同构.

线性代数中，K 向量空间 V 的线性变换就是把 V 看成带算集 K 的加群时的带算自同态.

于是，前面的 $a\to\bar{a}$ 就是 G 到 $\bar{G}$ 上的带算同态.

我们知道 G 的算子集中元可以看成 G 的自同态，由 $\sigma(\lambda(a))=\lambda(\sigma(a))$ 就有 $\sigma\lambda(a)=\lambda\sigma(a)$，因此 $\sigma\lambda=\lambda\sigma$. 于是，$G$ 的带算自同态 σ 能够与 G 的算子 λ 交换.

假如群的算子集是空集或者是恒等同态，那么它的子群都是带算子群，同构、同态也分别都是带算同构、带算同态，因此，§2.5 中定理对这种算子集言都一一成立，在一般情形时也能如此.

假如 G,G' 都是带算集 M 的群，σ 是 G 到 G' 上的带算同态，E 是 G' 的单位元 e' 的完全象源，也就是带算同态核. 因为 E 中任意元 $e_i\to e'$，那么

$$\lambda e_i\to\lambda e'=e',\lambda\in M,$$

所以 $\lambda e_i\in E$、于是 E 是 G 的带算正规子群. 因此 G 的象 $\sigma(G)$ 是 G' 的带算子群，σ 的同态核 E 是 G 的带算正规子群.

于是 §2.5 的定理 2 这时也成立. 又因为 $a\to\bar{a}$ 是 G 到 $\bar{G}$ 上的带算同态，所以 §2.5 的定理 4、定理 5 这时都一一成立. 再我们得知，当群是带算群时，只要子群，同构、同态等都是带算的，那么 §2.5 中的定理都能够一一成立. 此外，§3.3 的定理 1 这时也成立. 但要注意，因为带算单纯加群不一定是元数是质数的循环群，所以它的同态环一般只是体而不是域.

因为 R-模 M 是以 R 为带算集的加群，所以 M 的同态、同构指的都是带算同态、带算同构. 又因为 M 的子模都是带算的，所以这时 §2.5 中定理都能成立，也就是说对于模，§2.5 中定理都是能够成立的.

为了简便，在后面我们把"带算"两字一律省去不写，说群就是指带算群，因此子群、同构、同态等也都是指带算的而言，并且群的算子集都相同.

环对加法成群，因此对加法，它具备群的各种性质，但这只考

虑了加法而没有涉及另一个基本运算乘法，所以这样的性质不能显示环的特征．假如把环看成以自身为算子集的加群，这样既考虑了加法同时又考虑了乘法，得出的结果一般都是环的特性，因此带算群的理论在讨论环时是非常重要的．

要注意的是，环虽然可以看成以它的子集做算子集的带算加群，但是环的同态与带算加群的带算同态是有区别的．譬如，假定 a 是环 R 中元，那么

$$r \to ra$$

是把 R 看成用它的任一子集做算子集的加群时的带算自同态，当 a 是幂等元并且在 R 的中心 $Z(R)$ 时，才是环 R 的自同态．

下面是环的带算自同态的基本性质．

定理 1 假定 R 是有单位元 e 的环，τ 是把 R 看成以自身为(左)算子集的加群时的带算自同态，那么 R 中存在着唯一元 a，使

$$\tau(r)=ra, r\in R,$$

这就是说，R 的任意带算自同态与用 R 中某元右乘一致．

证明 假设 $\tau(e)=a$，因为 τ 是带算同态，所以

$$\tau(re)=r\tau(e)=ra,$$

即 $\tau(r)=ra$. 再假如 $\tau(r)=rb$，由 $ra=rb$，当 $r=e$ 时，即得 $a=b$. 因此定理成立．

由上面证明我们容易得知，当 e 是 R 的右单位元时，$\tau(r)=ra$ 仍然成立，只是 a 不是唯一的．

于是同§3.3习题8一样，我们容易证得

定理 2 假定 R 是有单位元的环，R' 是把 R 看成以自身为左算子集的加群的自同态环，那么 R 与 R' 逆同构．

同§4.1中一样，有时为了方便，我们把算子写在右边．写在左边的叫做左群，写在右边的叫做右群，凡是左群的性质能够同样证明也是右群的性质．

一般，假如群 G 有左算子集 M，同时又有右算子集 N，这时如果它们中元又满足

$$(\lambda a)\mu=\lambda(a\mu), a\in G, \lambda\in M, \mu\in N,$$

那么 G 叫做带算集 M,N 的群，或者叫做 M-N-群，当 $M=N$ 时，我们又叫 G 做 M-复群．

由定义容易得知，μ 可以看成 M-左群 G 的带算自同态，λ 可看成 N-右群 G 的带算自同态，因此如果 M,N 都是乘集，那么 N 与 M-左群 G 的自同态半群的子乘集逆同构，而 M 则与 N-右群 G 的自同态半群的子乘集同构．

M-N-群 G 的子群如果又是 M-N-群，它就叫做 G 的带算子群．M-N-群 G 到 M-N-群 G' 上的同态 σ，如果又满足

$$\sigma(\lambda a)=\lambda\sigma(a), \sigma(a\mu)=\sigma(a)\mu,$$

那么

$$\sigma(\lambda a\mu)=\lambda\sigma(a)\mu,$$

因此 σ 叫做带算同态．这时 § 2.5 中定理及 § 3.3 定理 1 都同样能够一一成立．

假如 R 是有单位元 e 的环，τ 是把 R 看成 R-复群时的带算自同态，因为 τ 也是把 R 看成以自身为左算子集加群时的带算自同态，由上面的定理 1，$\tau(r)=ra$．同样，因为 τ 又是把 R 看成以自身为右算子集加群时的带算自同态，所以

$$\tau(r)=\tau(er)=\tau(e)\cdot r=ar,$$

于是 $ra=ar$，这就是说，a 是 R 中与 R 的任意元能够交换的元，因此 a 在中心 $Z(R)$ 中．反过来 $Z(R)$ 中任意元显然决定 R 的一个带算自同态，于是 R 的带算自同态环与 $Z(R)$ 同构．

我们知道单环有单位元时，它的中心是域（§ 3.6 习题 10），于是我们有与 § 3.3 定理 1 类似的定理．

定理 3　有单位元的单环假如看成是自身的复群，那么它的带算自同态环是域．

同群一样，环也有所谓带算环，假如 R 是环，M 是集合，如果对于 M 中任意元 λ，R 中任意元 a,b，

$$\lambda a\in R, \lambda(a+b)=\lambda a+\lambda b, \lambda(ab)=(\lambda a)b=a(\lambda b),$$

即末 λ 叫做 R 的（左）算子，M 叫做 R 的（左）算子集，R 叫做带

(左)算集 M 的环，有时又叫做 M-环，因此 F 的代数就是 F-环．要注意的是这时 $a\to\lambda a$ 不是环 R 的自同态，这与关于群的不一致．

在讨论带算环时，我们就要考虑它的带算子环，带算理想以及带算同态、带算同构等，这些我们都不详细介绍了．

习 题 6.1

1. 试证带算同态把带算子群仍然变为带算子群．

2. 试证带算循环群的任意子群都是带算子群．

3. 试证带算对称群 S_4 的正规子群 A_4, B_4 都是带算正规子群．

4. 假如群 G 是带算群，那么它的换位子群 G' 是带算子群．

5. 在由有理数对 (a_1, a_2) 形成的环中（§3.1 习题 2），由 $(1,0)$ 及 $(0,1)$ 生成的两个理想是看成环时的同构，但不是看成加群时的带算同构，这是为什么？

6. 假如把域 F 的 n 维向量空间 V 看成为带算集 F 的加群，试证 V 的自同态环与全矩阵环 F_n 同构．

§6.2 同构定理

在§2.5 中我们介绍了群的一个同态基本定理，这节我们来介绍三个群的同构基本定理，它们在应用上都是很广泛的．为了简便，群的算子集都省略不写出，以后三节都是如此．

§2.5 的定理 5 是 G' 的单位元群与它的完全象源的一个重要关系，下面的第一同构定理就是表示这种关系对于 G' 中任意正规子群也能够同样成立，因此第一同构定理可以说是表示两个同态群间商群的同构关系．

定理 1 假定 G, G' 是群，$G\sim G'$，$H'\lhd G'$，那么 H' 在 G 中的完全象源 $H\lhd G$，并且

$$G/H\cong G'/H'.$$

证明 因为 $G\sim G'$，$G'\sim G'/H'$，所以 $G\sim G'/H'$．由第二

个同态关系，我们得知 G'/H' 的单位元在 G' 中的完全象源是 H'. 由假设，H' 在 G 中的完全象源是 H，因此 G'/H' 的单位元在 G 中的完全象源就是 H，也就是说 $G\sim G'/H'$ 时，同态核是 H. 于是由§2.5定理5，$H\lhd G$ 并且 $G/H\simeq G'/H'$，因此定理得证.

上定理显然是§2.5定理5的推广，因为假如 $H'=e'$，那么 E 就是 e' 的完全象源，G'/H' 就是 G'.

假如 $G\sim G'$，$H\lhd G$，H' 是 H 在 G' 中的象，因为同态把正规子群变为正规子群，所以 $H'\lhd G'$. 要注意的是，这时 H 不一定是 H' 的完全象源，因此 G/H，G'/H' 一般不是同构. 但它们是同态，即

$$G/H\sim G'/H'.$$

这是因为，我们把 G 分为 H 的陪集 a_iH，因为 $(a_iH)'=a_i'H'$，并且 $(a_ia_jH)'=a_i'a_j'H'$，所以 $a_iH\to a_i'H'$ 是 G/H 到 G'/H' 上的同态.

譬如假如 $a^{12}=1$，由 $(a)\sim(a^2)$ 我们容易得知 (a) 的子群 (a^4) 在 (a^2) 的象是 (a^4)，于是 $(a)/(a^4)\sim(a^2)/(a^4)$，$a\to a^2$ 是它的同态映射，因为 $(a)/(a^4)\simeq(a^3)$，$(a^2)/(a^4)\simeq(a^6)$ 两者元数不同，显然不同构，其原因是 (a^4) 在 (a) 的完全象源是 $(a^2)\supset(a^4)$.

怎样的象源才是完全象源？假定 $G\sim G'$，E 是它们的同态核，H' 是 G 的子群 H 在 G' 的象，H'' 是 H' 在 G 的完全象源. 因为 HE 的象是 H'，所以 $HE\subseteq H''$. 反过来，因为 H'' 中任意元 k 与 H 中某元 h 在 G' 中有相同的象，所以 $h^{-1}k$ 的象是单位元，于是 $h^{-1}k\in E$，即 $k\in hE$，因此 $H''\subseteq HE$，所以 $H''=HE$. 这就是说 H'' 是 H 与同态核 E 的乘积 HE. 假如 $H\supseteq E$，那么 H 就是 H' 的完全象源了.

假如 K，H 都是群 G 的正规子群，并且 $K\supseteq H$，因为

$$G\sim G/H,$$

而 K 在 G/H 中的象是 K/H，所以 K/H 是 G/H 的正规子群. 又因为 K/H 在 G 中的完全象源是 K，由定理1，我们有

(1) $$G/K\simeq(G/H)/(K/H).$$

下面是我们的**第二同构定理**，它表示一个群中两个子群的积与它们的交之间的同构关系．

定理 2 假设 H,K 是群 G 的子群，并且 $H\lhd G$ 那么 $K\cap H\lhd K$ 并且

$$KH/H\simeq K/(K\cap H).$$

证明 假定 K 在 $\bar{G}=G/H$ 的象是 $\bar{K}$，因为 $K\sim\bar{K}$，并且同态核是 $K\cap H$，所以 $\bar{K}\simeq K/(K\cap H)$．又因为 $G\sim\bar{G}$ 的同态核是 H，而 $\bar{K}$ 在 G 的完全象源是 KH，于是由 $KH\sim\bar{K}$，我们就有

$$\bar{K}\simeq KH/H,$$

因此定理成立．

譬如 $K=((1324))$，$H=B_4$（§2.3），因为

$KH=((12),(14)(23))$，$K\cap H=\{(1),(12)(34)\}$，

计算得 KH/H、$K/(K\cap H)$，皆元数是 2 的循环群，二者同构．

特别，当 $K\cap H$ 是单位元群时，我们即得

$$KH/H\simeq K,$$

也就是说，这时我们简直可以把 H 消去．

下面第三同构定理，是查生浩斯在 1934 年提出的，也叫做**查生浩斯定理**，它表示四个子群间的同构关系，是第二同构定理的推广．

定理 3 假设 K,H 是群 G 的子群，$K'\lhd K$，$H'\lhd H$，那么 $K'(K\cap H')\lhd K'(K\cap H)$，$H'(H\cap K')\lhd H'(H\cap K)$，并且

$$K'(K\cap H)/K'(K\cap H')\simeq H'(H\cap K)/H'(H\cap K').$$

证明 $K\cap H$ 及 $K'(K\cap H')$ 显然都是 $K'(K\cap H)$ 的子群．再 $K'(K\cap H')\lhd K'(K\cap H)$ 这是因为，假如 $k'u$ 是 $K'(K\cap H)$ 中任意元，这里 $k'\in K'$，$u\in K\cap H$，那么

$$\begin{aligned}k'u\cdot K'(K\cap H')\cdot u^{-1}k'^{-1}&=k'K'\cdot u(K\cap H')u^{-1}k'^{-1}\\&\subseteq K'(K\cap H')k'^{-1}\\&=K'k''(K\cap H')=K'(K\cap H').\end{aligned}$$

于是根据第二同构定理，我们有

$$K'(K\cap H')(K\cap H)/K'(K\cap H')$$
$$\simeq(K\cap H)/(K\cap H)\cap K'(K\cap H').$$

显然

$$(K\cap H')(K\cap H)=(K\cap H),$$

假如我们能够证明

$$(2)\qquad (K\cap H)\cap K'(K\cap H')=(K'\cap H)(K\cap H'),$$

那么

$$K'(K\cap H)/K'(K\cap H')\simeq(K\cap H)/(K'\cap H)(K\cap H').$$

因为在定理中，我们对于 K,K' 的要求，同对于 H,H' 的要求完全一样，假如在上式中把 K,K' 与 H,H' 互换，就得到

$$H'(H\cap K)/H'(H\cap K')$$
$$\simeq(K\cap H)/(K'\cap H)(K\cap H').$$

因此定理成立.

我们容易得知

$$(K'\cap H)(K\cap H')\subseteq(K\cap H),$$
$$(K'\cap H)(K\cap H')\subseteq K'(K\cap H'),$$
$$(K'\cap H)(K\cap H')\subseteq(K\cap H)\cap K'(K\cap H').$$

又假如 $a\in(K\cap H)\cap K'(K\cap H')$，那么 a 既属于 $K\cap H$，又属于 $K'(K\cap H')$，也就是说，

$$a=k'u,k'\in K',u\in K\cap H'.$$

因此，$k'\in H$，于是 $k'\in K'\cap H$，所以 $a\in(K'\cap H)(K\cap H')$，这就是说，

$$(K\cap H)\cap K'(K\cap H')\subseteq(K'\cap H)(K\cap H'),$$

于是(2)成立，因此定理得证.

特别，当 $K\supseteq H$，并且 H' 是单位元群时，我们就得到第二同构定理，因此第二同构定理是第三同构定理的特例.

显然这三个定理对 R-模也是成立的.

我们知道，理想对于环与正规子群对于群相类似，在上面三个

同构定理中，假如把群改为环，子群改为子环，正规子群改为理想，子群的积改为子环的和，那么这三个定理也都成立[1]. 譬如，环的第二同构定理就是：

假定 M，N 是环 R 的子环，N 是 R 的理想，那么 $M\cap N$ 是 M 的理想，并且 $(M,N)-N$ 与 $M-(M\cap N)$ 同构.

习 题 6.2

1. 试用第二同构定理证明对称群 S_4 关于 B_4 的商群 S_4/B_4 与 S_3 同构.

2. 试证在由排列但不全是偶排列组成的群中，所有偶排列形成指标是 2 的正规子群.

3. 假如 H，K 是群 G 的子群，$K'\lhd K$，试证 $H\cap K'\lhd H\cap K$，并且

$$(H\cap K)/(H\cap K')\simeq K/K' \text{ 的子群}.$$

4. 试证环的第二同构定理.

5. 试证任意有穷域与多项式环 $Z[x]$ 对于某理想 N 的同余环 $Z[x]-N$ 同构.

§6.3 正 规 群 列

在研究群时，常常要考虑它的正规子群，因此常常引用由正规子群及正规子群的正规子群组成的正规子群列. 这节我们详细地讨论这种重要的子群列.

群 G 的有穷个子群 G_i 组成的子群列

$$G=G_0\supset G_1\supset\cdots\supset G_k=E \tag{1}$$

叫做 G 的**正规群列**，k 叫做这正规群列的长，这里 E 是 G 的单位元群，$G_i\lhd G_{i-1}$.

除单位元群外，任意群显然都有正规群列. 譬如 $G\supset E$ 就是 G 的正规群列. 假如 G 不是单群，H 是异于 G 及 E 的正规子群，那么 $G\supset H\supset E$ 也是 G 的正规群列.

商群列 $\qquad G/G_1, G_1/G_2, \cdots, G_{k-1}/E$

叫做正规群列(1)的**商群列**.

显然有穷群的商群列中群都是有穷群，反过来也成立，即一个群如果它的商群列中群都是有穷群，那么这群也是有穷群．

假如

$$(2) \qquad G=H_0\supset H_1\supset\cdots H_l=E$$

又是 G 的正规群列，如果 G 的正规群列(1)中任意子群 G_i 与(2)中某子群 H_j 相等，也就是说，(1)中任意子群都包含在(2)中，那么(2)叫做(1)的**加细**，显然这时 $k\leqslant l$. 一个正规群列也可以看成是自身的加细．

一个正规群列如果没有异于自身的加细，就叫做**合成群列**．

显然，有穷群是有合成群列的．一个正规群列有时可以加细成为合成群列，譬如 $(a)\supset(a^2)\supset(a^6)\supset E$ 就是加细 $(a)\supset(a^2)\supset E$ 形成的合成群列．但也有时不论如何加细终不能使它成为合成群列的，譬如 $G=(a)$ 是无穷循环群，

$$G\supset G_1\supset\cdots\supset G_{k-1}\supset G_k=E$$

是它的任意正规群列，如果 $G_{k-1}=(a^m)$，那么 G_{k-1}、E 之间还存在着正规子群 (a^{2m})，所以这时不论如何加细不能使这正规群列成为合成群列．这就是说，无穷循环群 (a) 没有合成群列．因此任一群不一定都有合成群列，一个正规群列也不一定都能够加细成为合成群列．

下面，我们来讨论正规群列是合成群列的必要充分条件．我们先介绍与§3.8中极大理想类似的重要概念以备引用．

假如 G 是群，$H(\neq G)$ 是它的正规子群，如果 G 中除 G 及 H 自身外，不再有包含 H 的正规子群，那么 H 就叫做 G 的**极大正规子群**．譬如 n 个文字上的交代群 A_n 就是对称群 S_n 的极大正规子群．假如 $H\lhd G$, $\bar{G}=G/H$，如果 H 是极大正规子群，那么 $\bar{G}$ 是单群．这是因为，假如 $\bar{G}$ 中有异于自身及单位元群的正规子群 $\bar{K}$，因为 $G\sim\bar{G}$，由第一同构定理，$\bar{K}$ 在 G 的完全象源 $K\lhd G$，显然这时 $G\supset K\supset H$，这与 H 是极大的假设不合．反过来，假如 $\bar{G}$ 是单群，因为正规子群的同态象仍为正规子群，所以 G 中除 G 及 H 外没

有包含 H 的正规子群，因此 H 是极大正规子群．于是我们得到

定理 1 群 G 的正规子群 $H(\neq G)$ 是极大正规子群的必要充分条件是商群 G/H 为单群．

根据这定理，上面提出的问题不难立即解答．

假设(1)是 G 的正规群列，如果它是合成群列，那么 G_i 是 G_{i-1} 的极大正规子群，因此 G_{i-1}/G_i 是单群．反过来，如果 G_{i-1}/G_i 是单群，那么 G_i 是 G_{i-1} 的极大正规子群，因此它就是合成群列．于是我们有

定理 2 正规群列(1)是合成群列的必要充分条件是 G_{i-1}/G_i 是单群，或 G_i 是 G_{i-1} 的极大正规子群，$i=1,\cdots,k$.

由约当-赫尔特尔定理，这些单群 G_{i-1}/G_i 由 G 唯一决定．

一个群的两个正规群列，假如它们的长相等，依照某个顺序可以使第一个正规群列的商群与第二个正规群列的商群一对一的对应，并且所对应的商群又都同构，那么这两个正规群列叫做同构．

譬如元数是 6 的循环群 (a) 的两个正规群列

$$(a)\supset(a^2)\supset E,\ (a)\supset(a^3)\supset E$$

就是同构，这是因为它们的商群列都是由元数是 2 及 3 的两个循环群组成的．

一个群的任意两个正规群列显然不一定同构，下面我们来讨论它们加细的同构．

首先我们来考虑(1)，(2)如何加细其长才相等，商群依怎样的顺序能够同构？因为(1)的长是 k，(2)的长是 l，假如我们在(1)中每两个子群 G_{i-1}，G_i 之间都插 $l-1$ 个子群 G_{ij}，在(2)中每两个 H_{j-1}，H_j 之间都插 $k-1$ 个子群 H_{ij}，即假如有

$$G_{i-1}=G_{i0}\supseteq G_{i1}\supseteq\cdots\supseteq G_{il}=G_i,\ i=1,\cdots,k,$$

(3)

$$H_{j-1}=H_{0j}\supseteq H_{1j}\supseteq\cdots\supseteq H_{kj}=H_j,\ j=1,\cdots,l,$$

那么，这两个加细都包含 kl 个子群．再因为这时子群列(1)的加细是 k 个含有 l 个子群的组，子群列(2)的加细是 l 个含有 k 个子

群的组．假如前者第 i 组的 l 个商群顺次与后者各组的第 i 个商群同构，即

(4) $$G_{ij-1}/G_{ij} \simeq H_{i-1j}/H_{ij},$$

那么，上面这样的加细就是同构的了．

我们容易知道适合条件(4)的 G_{ij}, H_{ij}，当然也适合条件(3)，但是怎样来挑选适合条件(4)的这些 G_{ij} 及 H_{ij} 呢？因为

$$G_{i-1} \supseteq G_{ij} \supseteq G_i, H_{j-1} \supseteq H_{ij} \supseteq H_j,$$

我们可以取

$$G_{ij}=G_iK_{ij}, K_{ij} \subseteq G_{i-1}; H_{ij}=H_jL_{ij}, L_{ij} \subseteq H_{j-1}.$$

因此条件(4)就是条件

$$G_iK_{ij-1}/G_iK_{ij} \simeq H_jL_{i-1j}/H_jL_{ij}.$$

显然，根据第三同构定理，只要我们取

$$K_{ij}=G_{i-1} \cap H_j, L_{ij}=H_{j-1} \cap G_i$$

就行了，也就是说，我们取

$$G_{ij}=G_i(G_{i-1} \cap H_j), H_{ij}=H_j(H_{j-1} \cap G_i)$$

条件(4)就告成立．

再假如 $G_{ij-1}=G_{ij}$，那么 $G_{ij-1}/G_{ij}=E$. 因此 $H_{i-1j}=H_{ij}$. 反过来如果 $H_{i-1j}=H_{ij}$，那么 $G_{ij-1}=G_{ij}$.

于是，把这样的 G_{ij} 插入 G_{i-1}, G_i 之间，删去相等的得到长不大于 kl 的(1)的加细．把这样的 H_{ij} 插入 H_{j-1}, H_j 之间，删去相等的得到(2)的加细．这两个加细显然就是同构的了，因此我们有下面雪来义尔(O. Schreier, 1901～1929)定理．

定理 3 一个群的任意两个正规群列有同构的加细．

譬如 $G=(a)$ 是元数为 12 的循环群，

$$(a) \supset (a^2) \supset E, (a) \supset (a^3) \supset E$$

是它的两个正规群列，虽然长相等，但不同构．这时

$$G_0=H_0=(a), G_1=(a^2), H_1=(a^3), G_2=H_2=E.$$

于是我们有

$$G_{11}=G_1H_1=G_0, G_{21}=G_1 \cap H_1=(a^6),$$

$$H_{11}=H_1G_1=H_0, H_{12}=H_1\cap G_1=(a^6).$$

因此

$$(a)\supset(a^2)\supset(a^6)\supset E, (a)\supset(a^3)\supset(a^6)\supset E$$

是上面两个正规群列的同构加细．

据上定理，我们立即得到两个关于合成群列的主要定理．

定理 4　一个群的任意两个合成群列同构．

这定理叫做约当-赫尔特尔定理．因此，一个群如果有合成群列，那么它的合成群列的长是一定的，这长又叫做这群的长．

定理 5　一个群如果有合成群列，那么它的任意正规群列都能够加细成为合成群列．

引用正规群列，我们也可以把群来分类．

定义 1　群 G 假如它有商群都是交换群的正规群列，就叫做可解群．

显然，任意元数大于 1 的交换群都是可解群．交代群 A_5 不是可解群，因为它是非交换单群．

再我们容易证明交代群 A_2, A_3，对称群 S_2, S_3 都是可解群：又因为正规子群的象仍是正规子群，由 § 2.3，得知

$$S_4\supset A_4\supset B_4\supset C_4\supset E, C_4=\{1,(12)(34)\}$$

是对称群 S_4 的正规群列，它的商群

$$S_4/A_4, A_4/B_4, B_4/C_4, C_4$$

的元数分别是 2，3，2，2，它们都是质数，所以商群都是交换群，因此 S_4 是可解群．显然交代群 A_4 也是可解群．于是我们得知：当 n 不大于 4 时 A_n, S_n 都是可解群．

由上例，我们又可以知道，虽然交换群是可解群，但可解群不一定是交换群．此外，我们还可以知道，可解群的任意正规群列的商群也不一定都是交换群．譬如 S_4 的正规群列 $S_4\supset E$ 的商群 S_4 就不是交换群．但由定理 3 及上节的(1)式，它能够加细成为商群都是交换群的正规群列，因此，如果可解群有合成群列，那么，合成群列的商群都是交换单群．

我们知道，一个群如果其中任意有穷个元生成的子群都是有穷群，那么，这群叫做局部有穷群．交换周期群是局部有穷群．一般

定理 6 周期群如果又是可解群，那么它是局部有穷群．

证明 假定 G 是可解周期群，它的正规群列

$$G=G_0\supset G_1\supset\cdots\supset G_k=E,$$

的商群 G_{i-1}/G_i 都是交换群，因为 G 是周期群，所以 G_{i-1}/G_i 也是周期群，因此 G_{i-1}/G_i 是局部有穷群．于是假如 G_i 是局部有穷群，那么 G_{i-1} 也是局部有穷群（§2.5 习题 8）．但 G_{k-1} 是局部有穷群，所以 G 是局部有穷群．定理证毕．

我们知道 G 的换位子群是 $D(G)$，$D(G)$ 的换位子群我们就用 $D^2(G)$ 表示，因此 $D^{m+1}(G)$ 就是 $D^m(G)$ 的换位子群．于是，假如 $D^k(G)=E$，由 §2.3 定理 5，我们得知

$$G=D^0(G)\supset D(G)\supset\cdots\supset D^k(G)=E$$

是 G 的正规群列，并且它的商群都是交换群，因此这时 G 是可解群．反过来，假如 G 是可解群，它的正规群列

$$G=G_0\supset G_1\supset\cdots\supset G_k=E$$

的商群 G_{i-1}/G_i 都是交换群，因为 G/G_1 是交换群，由 §2.3 定理 5，G 的换位子群 $D(G)\subseteq G_1$，又因为 G_1/G_2 是交换群，所以 $D(G_1)\subseteq G_2$，但 $D^2(G)\subseteq D(G_1)$，所以 $D^2(G)\subseteq G_2$．一般我们有 $D^i(G)\subseteq G_i$．于是 $D^k(G)=E$．因此我们得下面可解群的必要充分条件．

定理 7 群 G 是可解群的必要充分条件是有某正整数 k，使 $D^k(G)=E$，即 G 有正规群列

$$G=D^0(G)\supset D(G)\supset\cdots\supset D^k(G)=E.$$

这里 k 叫做可解群的长．

显然，长是 1 的可解群是交换群，可解群只有长是 1 时才是交换群．因为当 $n\geqslant 5$ 时，交代群 A_n 的换位子群是它自身，所以不存在使 $D^k(A_n)=E$ 的 k，因此 $n\geqslant 5$ 时，A_n 不是可解群．

下面是可解群的重要性质．

定理 8 可解群的子群是可解群.

证明 假定 H 是可解群 G 的子群,因为

$$D^k(H) \subseteq D^k(G) = E,$$

即 $D^k(H) = E$,所以 H 是可解群,于是定理成立.

因为当 $n \geqq 5$ 时,交代群 A_n 不是可解群,所以对称群 S_n 也不是可解群. 于是我们得知 S_n, A_n,当 $n \leqq 4$ 时都是可解群,当 $n \geqq 5$ 时,都不是可解群.

定理 9 可解群的商群是可解群.

证明 假定 G 是可解群,$\overline{G} = G/H$ 是它的商群. 因为 $G \sim \overline{G}$,又因为换位子的象是换位子,换位子的象源中也有换位子,所以 G 的换位子群 $D(G)$ 在 $\overline{G}$ 的象是 $\overline{G}$ 的换位子群 $D(\overline{G})$,即

$$\overline{D(G)} = D(\overline{G}).$$

因此

$$D(G) \sim D(\overline{G}).$$

但 $D^k(G) = E$,所以 $D^k(\overline{G}) = \overline{E}$. 于是 $\overline{G}$ 是可解群,因此定理成立.

元数是 $p^a q^b$(p, q 是不相等的质数)的群是可解群[2],这是著名的伯恩赛德定理. 但元数是 $p^a q^b r^c$ 的群一般不是可解群,譬如 A_5 不是可解群,它的元数 $60 = 2^2 \cdot 3 \cdot 5$.

最后,我们介绍一类重要的可解群.

假定 H 是群 G 的正规子群,那么由所有形如

$$[g, h] = g^{-1}h^{-1}gh, g \in G, h \in H$$

的换位子生成的子群,我们用 $[G, H]$ 表示,显然 $[G, G] = D(G)$. 因为 $H \lhd G$,所以 $[g, h] \in H$,因此 $[G, H] \subseteq H$. 同§2.3中一样,对于任意元 $b \in [G, H]$,我们有 $gbg^{-1}b^{-1} \in [G, H]$. 于是 gbg^{-1} 属于 $[G, H]$,所以 $[G, H]$ 是 G 的正规子群.

定义 2 假定 G 是群,$G^{(1)} = [G, G]$,$G^{(i)} = [G, G^{(i-1)}]$,如果存在某正整数 m,使 $G^{(m)} = E$,那么 G 叫幂零群.

显然交换群是幂零群.

定理 10 p 群(§2.3)是幂零群.

证明 假定群 G 的元数是 p^n,我们对 n 用归纳法来证明. 当

$n=1$ 时，G 是循环群，显然 G 是幂零群，即这时定理成立．因为 G 的中心 $Z(G)$ 的元数大于 1（§2.4 习题 7），所以 $\overline{G}=G/Z(G)$ 的元数是 $p^k, k<n$．根据归纳法假设，$\overline{G}$ 是幂零群．于是我们有 $\overline{G}^{(m)}$ 等于 $\overline{E}$．但 $G\sim\overline{G}$，而 $G^{(m)}$ 的象是 $\overline{G}^{(m)}$，因此 $G^{(m)}\subseteq Z(G)$，再因为 $Z(G)$ 是交换群，它是幂零群，于是我们有

$$G^{(m+1)}\subseteq(Z(G))^{(1)}=E,$$

即 $G^{(m+1)}=E$，所以 G 是幂零群，于是定理成立．

同前面一样，假如 H 是群 G 的子群，由定义我们容易得知，$[H,H^{(i-1)}]\subseteq[G,G^{(i-1)}]$，即 $H^{(i)}\subseteq G^{(i)}$．因此，如果 G 是幂零群，那么 H 也是幂零群．再如果 $H\lhd G$，由 $G\sim\overline{G}=G/H$，我们也不难得知 $G^{(i)}\sim\overline{G}^{(i)}$．因此如果 G 是幂零群，那么 $\overline{G}$ 也是幂零群．于是我们有

定理 11 幂零群的子群是幂零群，幂零群的商群也是幂零群．

定理 12 幂零群是可解群．

证明 假定 G 是幂零群，$G^{(m)}=E$，因为

$$D(G)=G^{(1)}, D(G^{(1)})=[G^{(1)},G^{(1)}]\subseteq[G,G^{(1)}]=G^{(2)},$$

所以

$$D^2(G)=D(G^{(1)})\subseteq G^{(2)},$$

一般 $D^i(G)\subseteq G^{(i)}$，但 $G^{(m)}=E$．所以 $D^m(G)=E$，于是 G 是可解群．

定理的逆不一定成立；譬如对称群 S_3 是可解群，但不是幂零群．这是因为

$$D(S_3)=A_3, D^2(S_3)=D(A_3)=E,$$

但 $S_3^{(1)}=[S_3,S_3]=A_3$，$S_3^{(2)}=[S_3,A_3]=A_3$，却有 $S_3^{(1)}=S_3^{(2)}$．

1950 年华罗庚曾经证明非可换体的乘群不是可解群[3]．1961 年怀特与汤卜生证明了元数是奇数的群都是可解群[4]，这是一个重要的结果．

与上面类似，对于环也有合成环列，即环 R 的子环列

$$R=R_0\supset R_1\supset\cdots\supset R_k=0,$$

其中 R_i 是 R_{i-1} 的极大理想，叫做环 R 的合成环列．并且一个环的任意两个合成环列也同构，也就是说，R 的任意两个合成环列的项数相等，并且它们的同余环按某顺序彼此同构．

同样，域也有所谓合成域列，域 K 的子域列

$$K=K_0\supset K_1\supset\cdots\supset K_l=F,F\text{ 是质域},$$

其中 K_{i-1} 是 K_i 的正规扩张域、并且各域间不存在真中间正规扩张域，叫做 K 的合成域列．假如 K_{i-1} 关于 K_i 的次数是 n_i，那么

$$n_1,\cdots,n_l$$

叫做 K 的次数列．当次数列中数都是质数时，K 就叫做可解域．

习　题　6.3

1．试证对称群 S_2，S_3 都是可解群．

2．假如 G/H 是可解群，H 是可解群，那么 G 也是可解群．

3．假如 H，K 都是群 G 的子群，并且 K 是正规子群，如果 H，K 都是可解群，那么 HK 也是可解群．

4．假如 G 是群，试证 $D^k(G)$ 都是 G 的正规子群．

5．试求对称群 S_4 的所有合成群列．

6．假如交换群 G 有合成群列，那么 G 是有穷群．

7．试证 $[S_4,A_4]=A_4$，$[S_4,B_4]=B_4$．

8．试证 4 元数群是幂零群．

9．假定 N 是 G 的子群，$N\subseteq Z(G)$，如果 G/N 是幂零群，那么 G 也是幂零群．

10．试证 $Q(\sqrt[4]{2},i)$ 是可解体，这里 Q 是有理数域．

11．一个群，如果它有商群都是循环群的正规群刊，那么它就叫做超可解群．对称群 S_3 是超可解群，但不是幂零群，因此，超可解群是界于可解群与幂零群之间的一类群，试证超可解群的子群及商群都是超可解群[5]．

§6.4　直　　积

在群论中，直积是一个重要概念，它把一个群用构造比它简单

的子群来表达,在讨论群的构造时起着重大作用,这节介绍它的基本概念及简单性质.

由§2.3我们知道,假如群 G 是它的两个子群 A,B 的乘积,即 $G=AB$,那么 G 中任意元能够用 $ab,a\in A,b\in B$,来表示.但是这表示一般不是唯一的,并且 G 的结合法不一定能够用 A,B 的结合法来完全决定.如果 A,B 满足某些条件,这要求是可以达到的.这样,我们就有了直积这个概念.

假定 A,B 是群 G 的子群,如果

1° $A\lhd G,B\lhd G$;

2° $G=AB$;

3° $A\cap B=E$,E 是 G 的单位元群,

那么 G 叫做子群 A,B 的直积,用记号 $G=A\times B$ 来表示.这时我们又说 G 能够分解为 A,B 的直积,A,B 叫做 G 的**直积因子**.

显然 $S_3,A=((12)),B=((123))$ 适合条件2°,3°,但不适合1°,因为 S_3 不是 A,B 的直积.

当 G 是加群时,如果 G 是 A,B 的直积,我们就用 $G=A+B$ 来表示,叫 G 做 A,B 的直和,A,B 叫做 G 的**直和因子**.因为模是带算加群,所以模同样也有直和、直和因子等概念.

定理1 群 G 是它的子群 A,B 的直积的必要充分条件是:

1° G 中任意元 g 能够唯一地表为

$$g=ab,a\in A,b\in B;$$

2° A 中任意元与 B 中任意元能够交换.

证明 假如 G 是它的子群 A,B 的直积,因为对于 G 中任意元 g,我们有 $g=ab$,如果

$$g=a_1b_1=a_2b_2,a_1,a_2\in A;b_1,b_2\in B,$$

那么 $a_2^{-1}a_1=b_2b_1^{-1}$.但 $A\cap B=E$,于是

$$a_2^{-1}a_1=b_2b_1^{-1}=e,e\text{ 是 }G\text{ 的单位元},$$

所以 $a_1=a_2,b_1=b_2$.因此 $g=ab$ 这种表示是唯一的(1°).

再因为 $A\lhd G,B\lhd G$,所以

$$aba^{-1}b^{-1}=a(ba^{-1}b^{-1})=(aba^{-1})b^{-1}$$

是 A 中元，同时也是 B 中元，于是

$$aba^{-1}b^{-1}=e,$$

所以 $ab=ba$. 因此 A 中任意元与 B 中任意元能够交换(2°).

总之必要条件成立.

再假如定理中 1°, 2°两条件成立，因为对于 G 中任意元 g，我们有 $g=ab$，所以 $G\subseteq AB$. 因此 $G=AB$. 又因为 A 中任意元与 B 中任意元能够交换，所以

$$gAg^{-1}=abAb^{-1}a^{-1}=aAa^{-1}\subseteq A,$$

因此 $A\lhd G$. 同样 $B\lhd G$. 再假如 $c\in A\cap B$，那么

$$c=e\cdot c=c\cdot e.$$

因为这种表示是唯一的，所以 $c=e$，于是 $A\cap B=E$，因此 G 是 A, B 的直积. 所以充分条件成立. 定理证毕.

如果 G 是加群，2°是显然的，因此只需要条件 1°.

假如 G 是子群 A, B 的直积，g_1, g_2 是 G 中任意元，

$$g_1=a_1b_1, g_2=a_2b_2,$$

那么 $g_1g_2=a_1a_2\cdot b_1b_2$. 这就是说，$G$ 中任意两元相乘，只要乘它们的因子就行了. 因此，假如 A, B 的构造已经知道，那么 $G=A\times B$ 的构造也就知道，也就是说，G 的构造能够由 A, B 的唯一决定. 当 G 是有穷群时

$$|G|=|A|\cdot|B|,$$

即 G 的元数等于它的直因子的元数的乘积.

譬如，6 元循环群 (a) 是子群 (a^2), (a^3) 的直积，即

$$(a)=(a^2)\times(a^3).$$

又假如 G 是 15 元群，由西洛第二定理(§2.4)，G 只有 1 个 3 西洛子群 G_1，也只有 1 个 5 西洛子群 G_2，因此它们都是 G 的正规子群，显然都是循环群，即 $G_1=(a)$, $G_2=(b)$. 于是

$$G=G_1\times G_2=(a)\times(b)=(ab).$$

因此 G 是循环群. 就是说，15 元群除同构的外只是一个循环群.

一个群的构造如何用它的子群的构造来决定，这是一个重要问题，再一个群有多少个互不同构的类，也就是同构分类，也是一个重要问题，这些都可以引用直积来完成，直积之所以重要主要也就在此．

由定义我们容易得知，假如 $G=A\times B$，显然 $G=B\times A$. 再根据第二同构定理，我们有

$$A\simeq G/B,B\simeq G/A.$$

这就是说，假如 $G=A\times B$，那么 A 是 $G\sim G/A$ 的同态核，并且这同态又是 B 与 G/A 的同构．因此 G 是与它的同态象同构的子群与同态核的直积．反过来，假如 A 是群 G 的某同态的同态核，并且这同态又是同态象与 G 的正规子群 B 的同构，如果 $G=AB$ 或 $A\cap B=E$，那么 $G=A\times B$. 这是因为如果 $G=AB$，那么 $B\simeq G/A\simeq AB/A\simeq B/A\cap B$ 所以 $A\cap B=E$. 因此 G 等于 $A\times B$. 如果 $A\cap B=E$，那么 $AB/A\simeq B/A\cap B\simeq B\simeq G/A$，所以 $G=AB$，因此 $G=A\times B$. 譬如 $G=(a)$，$a^8=1$，$G\sim(a^2)=B$，其同态核是 $(a^4)=A$. 显然 $G\neq A\times B$，这时 $G\neq AB$，并且 $A\cap B\neq E$.

关于直积因子，我们还有下面一个定理．

定理 2　假定 H 是群 G 的正规子群，如果 H 又是完全群（§2.3），那么

$$G=H\times Z(H),$$

即 H 是 G 的直积因子．

证明　因为 H 的中心是单位元群，所以 $H\cap Z(H)=E$，如果 $G=H\cdot Z(H)$，那么 $G=H\times Z(H)$，定理就告成立．

因为 H 的自同构 $gHg^{-1}=H$ 是 H 的某一内同构 $hHh^{-1}=H$，即 $a_i\to ga_ig^{-1}$ 是 $a_i\to ha_ih^{-1}$. 所以 $ga_ig^{-1}=ha_ih^{-1}$，$a_i\in H$，因此 $h^{-1}ga_i=a_ih^{-1}g$，于是 $h^{-1}g\in Z(H)$ 即 $g\in H\cdot Z(H)$，也就是 $G\subseteq H\cdot Z(H)$. 定理证毕．

一个群假如能够分解为真子群的直积，它的子群不一定也都能够分解为其真子群的直积，但是它的某些子群却能够如此．

定理 3 假如群 $G=A\times B$，那么 G 的中心 $Z(G)$ 是 A 的中心 Z_1 与 B 的中心 Z_2 的直积：

$$Z(G)=Z_1\times Z_2.$$

证明 因为 $G=A\times B$，显然 Z_1 中任意元与 Z_2 中任意元的乘积是 $Z(G)$ 中元．假如能够证明 $Z(G)$ 中任意元是 Z_1 中元与 Z_2 中元的乘积，那么 $Z(G)=Z_1\cdot Z_2$，再由定理 1，这定理就显然了．

根据假设 $Z(G)$ 中任意元 z 可以写成

$$z=ab, a\in A, b\in B.$$

设 a' 是 A 中任意元，由 $a'z=za'$，我们有

$$a'ab=aba'=aa'b,$$

于是 $a'a=aa'$，所以 $a\in Z_1$．同样 $b\in Z_2$，即 z 是 Z_1 中元与 Z_2 中元的乘积，定理证毕．

定理 4 假设群 $G=A\times B$，H 是 G 的子群，并且 $H\supseteq A$，那么

$$H=A\times(H\cap B).$$

证明 显然 $A(H\cap B)\subseteq H$，又因为 $H\subseteq G$，所以 H 中任意元 h 可以写成

$$h=ab, a\in A, b\in B.$$

但 $b=a^{-1}h\in H$，因此 $b\in H\cap B$，所以

$$H=A(H\cap B).$$

再因为 $A\lhd G, B\lhd G$，所以 $A\lhd H, H\cap B\lhd H$，又因为

$$A\cap(H\cap B)\subseteq A\cap B=E,$$

根据定义，H 是 $A, H\cap B$ 的直积，因此定理得证．

假如 G 是群，

$$G=A\times B=A_1\times B_1,$$

如果 $B\simeq B_1$，对任意 A，我们有

$$A\simeq A',$$

我们就说 B 能够从直积中消去．假如 G 是有穷循环群，显然 B 可以从直积中消去．1962 年卡普伦斯基(I. Kaplansky, 1917～)猜想当 B 是无穷循环群时，B 也可以从直积中消去．1967 年胡柯(L.

Fuchs)证明无穷循环群不能从直积中消去,否认了这个猜想.1969年伊桑(R. Hirshon)证明了当 B 是有穷群时,它可以从直积中消去;当 B 是无穷群时,如果它满足正规子群的极大条件,也可以从直积中消去,解答了这问题.1975年伊桑对这又有新结果,读者欲知其详,请参考文献[6].

在环中也有类似的消去问题,请参考文献[7].

上面两个子群直积的概念,我们可以推广如下.

假设 $A_1,A_2,\cdots,A_n$ 是群 G 的子群,如果

1° $A_1,A_2,\cdots,A_n$ 都是群 G 的正规子群;

2° $G=A_1A_2\cdots A_n$;

3° $B_i\cap A_i=E,B_i=A_1\cdots A_{i-1},i=2,\cdots,n,E$ 是单位元群,那么 G 叫做 $A_1,A_2,\cdots,A_n$ 的直积,即

$$G=A_1\times A_2\times\cdots\times A_n,$$

而 A_i 叫做 G 的直积因子.

同上面定理1一样,假如 G 是 $A_1,\cdots,A_n$ 的直积:

$$G=A_1\times\cdots\times A_n,$$

我们容易得知

1° G 中任意元 g 能够唯一地表为

$$g=a_1a_2\cdots a_n,a_i\in A_i.$$

2° A_i 中任意元与 $A_j,i\neq j$,中任意元能够交换.

反过来,如果上面1°、2°两条件成立,命

$$B_i'=A_1\cdots A_{i-1}A_{i+1}\cdots A_n,$$

那么 $G=A_i\times B_i'$.于是 $A_i\lhd G$ 并且因为 $A_i\cap B_i'=E$,所以 $A_i\cap B_i=E$,因此根据定义,G 是 $A_1,\cdots,A_n$ 的直积.这就是说:

上面两条件1°,2°是 G 是 $A_1,\cdots,A_n$ 的直积的必要充分条件.

当 G 是加群时,只要条件1°就行了.

要注意的是,假如 G 中任意元能够表为 $A_1,\cdots,A_n$ 中元的乘积,并且 A_i 中任意元与 $A_j,i\neq j$,中任意元又能够交换,这时只要对于 G 的单位元 e 这种表示是唯一的,那么对于 G 中任意元这种

表示也是唯一的．这是因为，如果

$$a_1a_2\cdots a_n=a'_1a'_2\cdots a'_n,$$

我们就有

$$a'_1a_1^{-1}a'_2a_2^{-1}\cdots a'_na_n^{-1}=e,$$

因此

$$a'_i=a_i, i=1,2,\cdots,n.$$

上面介绍直积的概念，现在我们来讨论直积的基本性质．

假如 $G=A_1\times A_2\times\cdots\times A_n$，如果

$$A'_1=A_1\times\cdots\times A_{n_1}, A'_2=A_{n_1+1}\times\cdots\times A_{n_1+n_2},\cdots,$$

$$A'_m=A_{n_1+\cdots+n_{m-1}+1}\times\cdots\times A_n,$$

那么我们有

(1) $$G=A'_1\times A'_2\times\cdots\times A'_m.$$

如果 $A_i=B_{i1}\times\cdots\times B_{im_i}$，由定义，我们又容易验证

$$G=B_{11}\times\cdots\times B_{1m_1}\times\cdots\times B_{n1}\times\cdots\times B_{nm_n},$$

这就是说，在若干个子群的直积中，与元素乘积的情况一样，我们可以任意添加括弧或减少括弧．

假如 $G=A_1\times A_2\times\cdots\times A_n$，命

$$G_i=A_1\times\cdots\times A_{n-i}, i=0,1,\cdots,n,$$

我们就得到 G 的正规子群列

(2) $$G=G_0\supset G_1\supset\cdots\supset G_n=E.$$

这时，如果 $G_{i-1}/G_i=A_{n-i+1}$ 有合成群列，命

$$A_i=A_{i0}\supset A_{i1}\supset\cdots\supset A_{ik_i}=E$$

是 A_i 的合成群列．于是我们有

(3) $$G_{n-i}=G_{n-i+1}A_{i0}\supset G_{n-i+1}A_{i1}\supset\cdots\supset G_{n-i+1}A_{ik_i}=G_{n-i+1},$$

我们容易得知 G_{n-i+1} 是 $G_{n-i+1}A_{ij-1}$ 及 $G_{n-i+1}A_{ij}$ 的正规子群，并且 $G_{n-i+1}A_{ij}\lhd G_{n-i+1}A_{ij-1}$，由第一同构定理，

$$G_{n-i+1}A_{ij-1}/G_{n-i+1}A_{ij}\simeq A_{ij-1}/A_{ij},$$

故 $G_{n-i+1}A_{ij-1}/G_{n-i+1}A_{ij}$ 是单群，于是上面的正规群列(2)用(3)加

细就得到G的合成群列．这是说，假如$G=A_1\times A_2\times\cdots\times A_n$，并且$A_i$都有合成群列，那么$G$也有合成群列，并且$G$的长等于$A_i$的长的和．

设V是体F的向量空间，因为V是带算集F的加群或F-模，如果它有由n个元形成的关于F的底，那么V的长是n，因此由§5.3约当-赫尔特尔定理，n是唯一的．这就是说，V关于F的底的元数是一定的．但是V中任意$(V:F)$个关于F线性无关的元形成它的底，所以V关于F的底的元数等于$(V:F)$，这就是§4.1中定理3不需要定理1、定理2的另一证明．

一个群如果能够分解为它的真子群的直积，就叫做**可分解群**，否则叫做**不可分解群**．譬如对称群S_n就是不可分解群(§2.3习题15)．再元数是质数幂的循环群，即循环p群以及无穷循环群也都是不可分解群．这是因为，它们的任意两个子群的交都异于单位元群．同样，模也是如此，假定$M(\neq 0)$是R-模，如果M不能分成为两个子模的直和，或者说M的直和因子只有0及M自身，那么M叫做**不可分解模**．否则M叫做**可分解模**．环R的左理想看成R-模时，如果又是不可分解模，叫做R的不可分解左理想．R的极小左理想是R的不可分解左理想．

一个群如果能够分解为它的真单子群的直积，就叫做**完全可分解群**．我们很容易知道，假如G是完全可分解群，它分解为n个单群的直积，那么它有长是n的合成群列，也就是说它的长是n．

下面是完全可分解群的基本性质．

定理5 假设G是完全可分解群，A是它的任意正规子群，那就存在一正规子群B，使得G是A，B的直积，即

$$G=A\times B.$$

这就是说，完全可分解群的任意正规子群是它的直积因子．

证明 假设$G=A_1\times\cdots\times A_n$，$A_i$是单群，那么

$$G=A\cdot A_1\cdots A_n.$$

因为 A_1 是单群，$A\cap A_1\lhd A_1$. 所以 $A\cap A_1$ 是 A_1 或者是单位元群 E. 当 $A\cap A_1=A_1$ 时，$AA_1=A$，这时我们把 A_1 删去；当 $A\cap A_1=E$ 时，$AA_1=A\times A_1$，这时我们把 AA_1 改写成 $A\times A_1$. 这样继续进行，一般因为 $(A\cdot A_1\cdots A_{k-1})\cap A_k$ 是单群 A_k 的正规子群，所以它是 A_k 或是 E，因此我们可以把 A_k 删去或把 $(A\cdot A_1\cdots A_{k-1})A_k$ 改写成 $(A\cdot A_1\cdots A_{k-1})\times A_k$. 假如把所有这些多余的 A_i 一一删去，把剩下的乘积改成直积，我们就得到

$$G=A\times A_{i_1}\times\cdots\times A_{i_r},$$

因此 $A_{i_1}\times\cdots\times A_{i_r}$ 就是所求的正规子群 B，所以定理得证.

在上面的证明中，假如把 $G=A_1\times\cdots\times A_n$ 中异于 $A_{i_1},\cdots,A_{i_r}$ 的直积因子的直积用 A' 表示，那么 $G=A'\times A_{i_1}\times\cdots\times A_{i_r}$，因此 $A\simeq A'$. 但 A' 是完全可分解群，所以 A 也是完全可分解群. 再假如 A 是完全可分解群 G 的正规子群，由 $G=A\times B$，我们有 $G/A\simeq B$. 因为 $B\lhd G$，所以是完全可分解群，因此 G/A 是完全可分解群. 于是我们有

定理 6 完全可分解群的正规子群是完全可分解群. 完全可分解群的商群也是完全可分解群.

由 §2.3，我们知道在一般群中，正规子群这个关系是不适合传递律的，但在完全可分解群中，传递律能够成立. 这是因为，完全可分解群的正规子群是它的直积因子. 再由定义我们容易证明，任意直积因子的正规子群仍然是群的正规子群. 因此，假如 G 是完全可分解群，如果 $A\lhd B$，$B\lhd G$ 那么 $A\lhd G$.

在 §3.9，我们讨论了元素的分解，这里我们介绍群的分解. 一个群在什么条件下能分解为不可分解群的直积，在什么条件下这种分解又是唯一的？对此，克努尔，雷马克(R. Remak)，许密特(E. Schmidt，1845～1921)有一个重要定理：

假定群 G 满足正规子群的降链条件(§7.1)，那么 G 能够分解为有穷个不可分解子群的直积. 假如 G 满足正规子群的降链条件及升链条件，那么 G 能够唯一的分解为有穷个不可分解子群

的直积，即如果

$$G=G_1\times\cdots\times G_h, G=H_1\times\cdots\times H_k,$$

G_i, H_i 都是不可分解子群，那么 $h=k$. 并且适当的改变顺序可以使 $G_i\simeq H_i$. 它的证明当然从略，请参考文献[8].

上面是讨论在同一群中若干个子群的直积，任意若干个群的直积，我们也可以仿照上面的方法来定义.

假定 A, B 是两个群(相等或不相等)，我们取所有元素对

$$(a,b), a\in A, b\in B,$$

并且规定 $(a_1,b_1)=(a_2,b_2)$，当 $a_1=a_2, b_1=b_2$，

$$(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2),$$

$$\lambda(a,b)=(\lambda a,\lambda b), \lambda \text{ 是 } A, B \text{ 的算子}.$$

那么，所有这样元素对组成为群 G，单位元是 (e,e)，这里 e 是 A, B 的单位元，(a,b) 的逆元是 (a^{-1},b^{-1}). 再所有形如 (a,e) 及 (e,b) 的元素对分别成为与 A, B 同构的子群 A', B'. 显然 A', B' 是 G 的正规子群. 根据直积定义，我们容易证明 G 是子群 A', B' 的直积，这时我们把 A', B' 分别看成 A, B，因此 G 就是 A, B 的直积，即 $G=A\times B$.

显然，当 A, B 都是交换群时，$G=A\times B$ 也是交换群. 假如我们把 (a,b) 与 (b,a) 对应，即 $(a,b)\to(b,a)$，那么这对应就是 $A\times B$ 到 $B\times A$ 上的同构，因此 $A\times B\simeq B\times A$. 再因为 $((a,b),c)\to(a,(b,c))$ 是 $(A\times B)\times C$ 到 $A\times(B\times C)$ 的同构，于是 $(A\times B)\times C\simeq A\times(B\times C)$，所以我们有

$$A\times B=B\times A, (A\times B)\times C=A\times(B\times C),$$

即直积因子适合乘法的交换律及结合律.

为了方便，我们又常常把 (a,b) 写成普通乘积的形状 ab，即

$$(a,b)=ab,$$

因此 $a_1b_1=a_2b_2$，当 $a_1=a_2, b_1=b_2$，

并且 $(a_1b_1)(a_2b_2)=(a_1a_2)(b_1b_2)$，

$$\lambda(ab)=\lambda a\cdot\lambda b.$$

关于 n 个群 $A_1, \cdots, A_n$ 的直积 $A_1 \times \cdots \times A_{n-1} \times A_n$ 我们可以同样定义.

对无穷多个群也能如此. 假定有一组群 $\{G_i | i \in I\}$，这里 I 是任意集合可数的或不可数的. 那么所有形如

(1) $$(x_i | x_i \in G_i)$$

的元集合，结合法同前面一样，即

$$(x_i)(y_i) = (x_i y_i), \lambda(x_i) = (\lambda x_i), x_i, y_i \in G_i.$$

λ 是算子，形成为群，叫做 $\{G_i\}$ 的**完全直和**，如果(1)中 x_i 不为 G_i 的单位元的只有穷个，由所有这样元形成的群，叫做 $\{G_i\}$ 的**直和**，有时又叫做**离散直和**. 显然后者是前者的子群，当 I 是有穷集时，两者是一致的. 要注意的是两者不只是形式上有所别，有些基本性质也不完全一致.

因为模是带算加群，所以我们同样有两种直和. 一般前者叫直和，后者叫**直积**，当考虑的模只是有穷个时，直积与直和是一致的.

与群的直积类似，我们有环的**直和**.

假定 $R_1, R_2, \cdots, R_n$ 是 n 个环，那么所有形如 $(a_1, \cdots, a_n), a_i \in R_i$，的元，根据下面的结合法：

$$(a_1, \cdots, a_n) = (a'_1, \cdots, a'_n), \text{当 } a_i = a'_i, i = 1, \cdots, n$$

$$(a_1, \cdots, a_n) + (a'_1, \cdots, a'_n) = (a_1 + a'_1, \cdots, a_n + a'_n),$$

$$(a_1, \cdots, a_n) \cdot (a'_1, \cdots, a'_n) = (a_1 a'_1, \cdots, a_n a'_n),$$

成为一个环 R，其中所有形如 $(0, \cdots, a_i, \cdots, 0), a_i \in R_i$，第 j 个 0 是 R_j 的零元，的元形成与 R_i 同构的子环 R'_i，这 R 我们就叫做它的子环 $R'_1, \cdots, R'_n$ 的直和，我们把 R'_i 看成 R_i，因此 R 就是 $R_1, \cdots, R_n$ 的直和，写成

$$R = R_1 + \cdots + R_n$$

我们也常常把 $(a_1, \cdots, a_n)$ 写成和的形状 $a_1 + \cdots + a_n$，即

$$(a_1, \cdots, a_n) = a_1 + \cdots + a_n.$$

因此，$(a_1 + \cdots + a_n) + (b_1 + \cdots + b_n) = (a_1 + b_1) + \cdots + (a_n + b_n)$，

$$(a_1+\cdots+a_n)\cdot(b_1+\cdots+b_n)=a_1b_1+\cdots+a_nb_n.$$

同群的情况一样，我们容易证明这时 R_i 是 R 的理想，并且 $R_iR_j=0, i\neq j$.

假如环 R 看成加群时是它的理想 $R_i, i=1,\cdots,n$，的直和，那么环 R 也是子环 R_i 的直和．这是因为加群 R 是子加群 R_i 的直和，所以上面的规定中前两个条件成立，再因为 R_i 是 R 的理想，所以由 $R_i\cap R_j=0$，我们就有 $R_iR_j=0, i\neq j$. 于是上面第三个条件也成立．因此 $R=R_1+\cdots+R_n$.

同群的情况一样，$R=R_1+\cdots+R_n$ 时，R 中元能够唯一地表为 $R_1,\cdots,R_n$ 中元的和，再 R 的结合法能够由 R_i 的结合法唯一决定．因此引用直和，一个环可以化为构造比它简单的环来研究，譬如，$\bar{Z}_6=Z-(6)$ 显然不是体，但它是体 $\bar{Z}_2=Z-(2)$，$\bar{Z}_3=Z-(3)$ 的直和，即 $\bar{Z}_6=\bar{Z}_2+\bar{Z}_3$. 显然，$R_i$ 的理想也是 R 的理想．此外，在若干个子环的直和中，我们也可以任意增加或减少括弧．

一个环假如能够分解为真子环的直和，叫做**可分解环**，否则就叫做**不可分解环**．显然，单环是不可分解环，质环也是不可分解环．

下面环的两个性质与群的类似，不是一般环所具备的．

定理7 假如 $A(\neq R)$ 是环 R 中有单位元的理想，那么 R 是 A 及另一理想 B 的直和，即 $R=A+B$，并且 B 由 A 唯一确定．

证明 假定 e 是 A 的单位元，那么

$$B=\{r\mid r\in R, re=er=0\}$$

形成 R 的理想．显然 $A\cap B=0$. 再假如 r 为 R 中任意元，因为 $(re)e=re\in A$，命 $re=a$，得 $re=ae$，于是 $(r-a)e=0$. 再因为 e 是 A 的单位元，$er\in A$，所以 $ere=er$，即 $e(r-a)=0$. 因此 $r-a\in B$. 命 $r-a=b$，我们有 $r=a+b$. 于是 R 看成加群时是 A,B 的直和，因此 $R=A+B$.

再假定 $R=A+C$，c 是 C 中任意元，

$$c=a+b, a\in A, b\in B$$

因为 C 是 R 的理想，所以 $ce\in C$，又因为

$$ce=ae+be=ae=a,$$

所以 $a=0$；因此 $c=b$，即 $C\subseteq B$，同样 $B\subseteq C$ 所以 $B=C$，因此 B 由 A 唯一确定．于是定理成立．

于是环 R 中有单位元的理想是它的直和因子．

定理 8 假如 R 是有单位元 e 的环，并且是子环 $R_1,\cdots,R_n$ 的直和，即 $R=R_1+\cdots+R_n$，如果 L 是 R 的左理想，那么

$$L=L_1+\cdots+L_n,$$

这里 $L_i=R_i\cap L$.

证明 首先因为 R_i 都是 R 的理想，并且 $L_i\subseteq R_i$，所以 L_i 都是 L 的理想．又因为 R 是 $R_1,\cdots,R_n$ 的直和，$L_i\subseteq R_i$，如果 L 中元能够写成 $L_1,\cdots,L_n$ 中元的和，显然 L 就是 $L_1,\cdots,L_n$ 的直和了．

再因为 $$e=e_1+\cdots+e_n, e_i\in R_i,$$

所以对于 L 中任意元 a，我们有

$$a=ea=e_1a+\cdots+e_na.$$

由于 $a\in L\subseteq R$，所以 $e_ia\in R_iR=R_i$；又由于 $e_i\subset R_i\subset R$，所以 $e_ia\in RL=L$. 于是 $e_ia\in R_i\cap L=L_i$，这就是说，L 中任意元能够表为它的理想 $L_1,\cdots,L_n$ 中元的和．于是定理成立．

显然，当 K 是 R 的右理想时，定理同样成立，这就是说，在有单位元的可分解环中，左理想，右理想都是可分解环．

要注意的是，在上定理中有单位元这条件不可少，假如没有单位元，定理不成立．譬如设环 $R=R_1+R_1$ 其中 $R_1=\{\bar{0},\bar{2},\bar{4},\bar{6}\}$，$\bar{8}=\bar{0}$. 那么 $L=\{(\bar{0},\bar{0}),(\bar{4},\bar{4})\}$ 是 R 的理想．我们容易得知 L 不是 R 的直和因子，并且 L 也不是 R_1 的理想的直和．

再要注意的是，环的直和与把它看成以自身为左(右)模的直和是不相同的，前者的直和因子都是理想而后者是左(右)理想．

上面环的直和是对有穷个环面言，对无穷多个环也是如此，设有一组环 $\{R_i\mid i\in I\}$，那么所有形如 $(a_i\mid a_i\in R_i)$ 的元结合法同前面一样：即两元和的分量是它们分量的和、两元积的分量是它们分量

的积形成的环 R 叫做$\{R_i\}$的**完全直和**．如果我们再规定元中分量 a_i 不为零的只有穷个，这时$\{R_i\}$的直和有时又叫做**离散的**．我们容易得知，这时 R 中任意元是有穷个 R_i 中元的和．对于有穷个环，完全直和与离散直和是一致的．

习 题 6.4

1. 假设(a)是元数 $n=rs$ 的循环群，其中$(r,s)=1$，试证(a)是元数为 r 的循环群(a^s)与元数为 s 的循环群(a^r)的直积．

2. 假如循环群 A,B 的元数分别为 m,n，试证 $A\times B$ 是循环群的必要充分条件是 m,n 互质，即$(m,n)=1$.

3. 试求两个 3 元群的直积．

4. 假如群 $G=A\times B$，试证$[G,G]=[A,A]\times[B,B]$.

5. 假如 H 是交换群 G 的子群，G/H 是无穷循环群，试证
$$G=H\times G/H.$$

6. 假设 A,B 是群 G 的正规子群，$G=AB$，$H=A\cap B$，试证
$$G/H\simeq A/H\times B/H.$$

7. 假如 A,B 是群 G 的正规子群，试证
$$AB \text{ 的长}+A\cap B \text{ 的长}=A \text{ 的长}+B \text{ 的长}.$$

8. 假设环 $R=R_1+\cdots+R_n$，试证 R 的中心
$$Z(R)=Z_1+\cdots+Z_n,\ Z_i \text{ 是 } R_i \text{ 的中心}.$$

9. 假定 L 是有单位元环 R 的单纯左理想，试证 L 是 R 的直和因子的必要充分条件是 $L^2\neq 0$[9]

10. 假如环 R 看成 R 左加群时是它的左理想 $L_1,\cdots,L_n$ 的直和，如果 e 是 R 的单位元，那么，$e=e_1+\cdots+e_n$，$e_i\in L_i$，$L_i=Re_i$，并且 e_ie_j 当 $i=j$ 时为 e_i，当 $i\neq j$ 时为 0. 如 $e_1,\cdots,e_n$ 这样的幂等元叫做**正交幂等元**．反过来也成立，即假如 $e=e_1+\cdots+e_n$，e_i 是正交幂等元，那么 $R=Re_1+\cdots+Re_n$.

11. 假如环有异于单位元的幂等元，那么这环为以此幂等元为单位元的理想与其他理想的直和．

§6.5 交 换 群

这节我们讨论交换群的构造，也就是讨论交换群如何唯一地

分解为不可分解群(循环 p 群，无穷循环群)的直积．§2.4 给出了循环群的同构分类，这节可以说是讨论交换群的同构分类．这节讨论的群都是交换群．我们先从较简单的 p 群开始．

定理 1 p 群能够分解为循环 p 群的直积．

证明 假定 G 的元数是 p^n，我们对 n 用归纳法来证明．$n=1$ 时，定理显然成立．假定 $<n$ 时定理成立，我们来证明 n 时定理也成立．

假定 a 是 G 中最大阶数 p^r 的元，那么 $\bar{G}=G/(a)$ 的元数 $\frac{p^n}{p^r}=p^{n-r}$，因此 $\bar{G}$ 也是 p 群．于是，根据归纳法假设就得到

(1) $$\bar{G}=(\bar{a}_1)\times\cdots\times(\bar{a}_m).$$

下面，我们来证明 $G=(a)\times(a_1)\times\cdots\times(a_m)$，这里 a_i 是 $\bar{a}_i$ 在 G 的某个象源，显然 a_i 的阶数都是 p 的幂，因此定理就告成立．

首先，对于 G 中任意元 g，由 $\bar{g}\in\bar{G}$，得

$$\bar{g}=\bar{a}_1^{r_1}\cdots\bar{a}_m^{r_m}=\overline{a_1^{r_1}\cdots a_m^{r_m}},$$

因此 $g=a^{r_0}a_1^{r_1}\cdots a_m^{r_m}$，这就是说，$g$ 是 $(a),(a_1),\cdots,(a_m)$ 中元的乘积．

再假如 $a^s a_1^{s_1}\cdots a_m^{s_m}=e$，因为 $\bar{a}$ 是 $\bar{G}$ 的单位元，即 $\bar{a}=\bar{e}$，所以

$$\overline{a_1^{s_1}}\cdots\overline{a_m^{s_m}}=\bar{e},$$

由(1)我们有

(2) $$\overline{a_i^{s_i}}=\bar{e},\ i=1,\cdots,m.$$

我们命 $\bar{a}_i$ 的阶数是 p^{t_i}，a_i 的阶数是 $p^{t'_i}$，显然 $t'_i\geq t_i$．如果 $t'_i=t_i$，也就是说，a_i 的阶数也是 p^{t_i}，由(2)我们有 $p^{t_i}|s_i$，于是 $a_i^{s_i}=e$，因此 $a^s=e$，根据定义，$G=(a)\times(a_1)\times\cdots\times(a_m)$，所以这时定理成立．如果 $t'_i\neq t_i$，因为 $\bar{a}_i$ 的象源 a_i 不是唯一的，假如我们能够另选 a_i' 代替 a_i，使 a_i' 的阶数为 p^{t_i}，即 a_i' 的阶数与 $\bar{a}_i$ 的阶数相等，那么 $G=(a)\times(a_1')\times\cdots\times(a_m)$，因此定理也同样成立．我们知道

$$\overline{a_i^{p^{t_i}}}=\bar{a}_i^{p^{t_i}}=\bar{e},$$

因此 $a_i^{p^{t_i}}\in(a)$，命 $a_i^{p^{t_i}}=a^{\lambda}$，$\lambda$ 是整数，由

$$a^{\lambda p^{r-t_i}}=(a_i^{p^{t_i}})^{p^{r-t_i}}=a_i^{p^r}=e,$$

我们就得到 $p^r|\lambda p^{r-t_i}$，即 $\lambda=\mu p^{t_i}$. 命 $a_i'=a_ia^{-\mu}$，那么

$$a_i'^{p^{t_i}}=a_i^{p^{t_i}}a^{-\mu p^{t_i}}=e,$$

所以 a_i' 的阶数是 p^{t_i}，于是定理得证.

定理 2 p 群 G 能够唯一地分解为循环 p 群的直积，也就是说，假如

$$G=(a_1)\times\cdots\times(a_h)=(b_1)\times\cdots\times(b_k),$$

那么 $h=k$，并且适当选取 $(b_1),\cdots,(b_k)$ 的顺序，可以使 $(a_i)\simeq(b_i)$，即 a_i 的阶数 p^{r_i} 与 b_i 的阶数 p^{s_i} 相等.

证明 分解的可能性已如上述，下面我们用反证法来证明分解的唯一性.

为了便于叙述，我们假定

$$r_1\geqslant r_2\geqslant\cdots\geqslant r_h, s_1\geqslant s_2\geqslant\cdots\geqslant s_k,$$

$$r_1=s_1,\cdots,r_{i-1}=s_{i-1};\quad r_i<s_i.$$

因为 $\quad G^{p^{r_i}}=(a_1)^{p^{r_i}}\times\cdots\times(a_h)^{p^{r_i}}=(a_1^{p^{r_i}})\times\cdots\times(a_h^{p^{r_i}}),$

所以 $G^{p^{r_i}}$ 的元数为

$$p^{r_1-r_i}\cdots p^{r_{i-1}-r_i}=p^{(r_1+\cdots+r_{i-1})-(i-1)r_i}.$$

同样，又因为 $G^{p^{r_i}}=(b_1^{p^{r_i}})\times\cdots\times(b_k^{p^{r_i}})$，所以 $G^{p^{r_i}}$ 的元数为

$$p^{s_1-r_i}\cdots p^{s_{i-1}-r_i}p^{s_i-r_i}\cdots=p^{(s_1+\cdots+s_{i-1}+s_i)-ir_i+\cdots}.$$

于是

$$r_1+\cdots+r_{i-1}-(i-1)r_i=s_1+\cdots+s_{i-1}+s_i-ir_i+\cdots.$$

因此 $r_i=s_i+\cdots$，即 $r_i\geqq s_i$，这与上面假设不合. 于是 $r_i=s_i$，因此 $h=k$. 所以定理成立.

譬如，克莱茵四元群 $G=\{e,a,b,ab\}$，那么

$$G=(a)\times(b)=(a)\times(ab)=(b)\times(ab).$$

p 群分解为循环 p 群的直积时，如果循环 p 群的阶数都是 p 就叫做初等交换 p 群，譬如上面的克莱茵四元群就是初等交换 p 群.

特别,假如 G 是元数 $n=p_1^{l_1}\cdots p_m^{l_m}$ 的循环群,因循环群的子群仍是循环群,所以 G 能够分解为 $p_i^{l_i}$ 元循环群 (a_i),$i=1,\cdots,m$,的直积:

$$G=(a_1)\times\cdots\times(a_m).$$

由定理3及定理2,我们有下面重要定理.

定理4 有穷交换群能够唯一地分解为循环 p 群的直积.

譬如,12元交换群是它的4元子群与3元子群的直积. 因为4元交换群如果不是循环群,它就是克莱茵4元群,也就是两个2元群的直积. 所以12元交换群有两种类型:一类是循环群,它是4元群与3元群的直积;另一类是非循环群,它是两个2元群与一个3元群的直积.

于是,有穷交换群的研究,就可以转化为循环 p 群的研究了.

上面讨论的是有穷交换群,现在我们来讨论无穷交换群的构造. 但是,一般的无穷交换群的构造非常复杂,下面我们只讨论由有穷个元生成的交换群,它是交换群中重要的一类.

要注意的是,由有穷个元生成的群如果是交换群,那么它的子群,也是由有穷个元生成的,如果不是交换群,它的子群就没有这性质,其证明从略,请参考文献[10].

再我们容易知道,假如有穷个生成元的阶数都是有穷,显然由它们生成的交换群是有穷群;就是由它们生成的非交换群,伯恩赛德也认为是有穷群,或者说,伯恩赛德认为周期群是局部有穷群,这是1902年伯恩赛德提出的一个猜想,是所谓的伯恩赛德猜想. 半个世纪来讨论这问题的虽然大有人在,但只是证实了某些特殊情况,直到1963年Д.С. 诺维柯夫提出否定的证明,因此伯恩赛德猜想得到否定的解答[11].

假如群 G 是由 n 个元生成,但不能由少于 n 个元生成,那么由 n 个元组成的生成元集,叫做 G 的**极小生成元集**. n 叫做 G 的**秩**. 一个群如果是由有穷个元生成,那么它就有极小生成元集. 极小生成元集不是唯一的,譬如循环群的生成元就不是唯一的.

关于一般有穷群的构造我们有：

定理 3 假定群 G 的元数是 n，把 n 分解为质数 p_i 幂的乘积：$n=p_1^{r_1}\cdots p_m^{r_m}$，那么 G 能够唯一地分解为 $p_i^{r_i}$ 元西洛子群 G_i 的直积：$G=G_{p_1}\times\cdots\times G_{p_m}$.

证明 假如 G_i 是 G 中所有适合 $x^{p_i^{r_i}}=e$ 的元 x 的集合，如果 $a^{p_i^{r_i}}=e,b^{p_i^{r_i}}=e$，因为 G 是交换群，显然 $(ab)^{p_i^{r_i}}=e$，所以 G_i 是 G 的子群，因此由 §2.3 定理 6，G_i 是 p 群，所以 $|G_i|$ 是 p_i 的幂．

下面我们根据定义来验证 G 是 $G_1,\cdots,G_m$ 的直积．

首先假设 $q_i=\dfrac{n}{p_i^{r_i}}$，那么 $q_1,\cdots,q_m$ 的最大公约数是 1，因此有整数 $\lambda_1,\cdots,\lambda_m$，使得

$$\lambda_1q_1+\cdots+\lambda_mq_m=1.$$

于是 G 中任意元 g 能够写成

$$g=g^{\lambda_1q_1+\cdots+\lambda_mq_m}=g^{\lambda_1q_1}\cdots g^{\lambda_mq_m}.$$

但

$$(g^{\lambda_iq_i})^{p_i^{r_i}}=(g^{q_ip_i^{r_i}})^{\lambda_i}=(g^n)^{\lambda_i}=e,$$

因此 $g^{\lambda_iq_i}\in G_i$. 这就是说，G 中任意元 g 能够表为 $G_i,i=1,\cdots,m$，中元的乘积．

再假如 G 的单位元 $e=g_1\cdots g_m,g_i\in G_i$，因为 $g_i^{p_i^{r_i}}=e$，所以

$$g_i^{q_j}=e,i\neq j,$$

于是

$$g_1^{q_i}\cdots g_i^{q_i}\cdots g_m^{q_i}=e,$$

即 $g_i^{q_i}=e$. 但 q_i 与 $p_i^{r_i}$ 互质，于是由 $\mu_iq_i+\upsilon_ip_i^{r_i}=1$，我们有

$$g_i=(g_i^{q_i})^{\mu_i}(g_i^{p_i^{r_i}})^{\upsilon_i}=e.$$

因此根据定义，G 是 $G_1,\cdots,G_m$ 的直积．因为 G_i 由 G 唯一决定，所以这分解是唯一的．

又比较 G 及 G_i 的元数得知 $|G_i|=p_i^{r_i}$，再 G 中 $p_i^{r_i}$ 元子群显然只有 G_i，因此 $G_i=G_{p_i}$，于是定理成立．

我们知道，一个群假如除单位元外，任意元的阶都是无穷时，叫做纯无穷群．下面我们先来讨论纯无穷群的构造．

定理 5 由有穷个元生成的纯无穷交换群能够唯一地分解为无穷循环群的直积．

证明 假如 $a_1,\cdots,a_n$ 是群 G 的这样一组极小生成元集，在它们之间满足象下面这种关系：

(3) $$a_1^{\lambda_1}\cdots a_n^{\lambda_n}=e,\ e \text{ 是 } G \text{ 的单位元},$$

的整数 λ_i 只有完全都是零，也就是它们是与 §4.1 中类似的线性无关，这时我们容易证明 G 中任意元 g 能够唯一地表为 $a_1^{r_1}\cdots a_n^{r_n}$：$g=a_1^{r_1}\cdots a_n^{r_n}$，于是

$$G=(a_1)\times\cdots\times(a_n),$$

这里 (a_i) 显然都是无穷循环群．因此，如果我们能够证明 G 的极小生成元集中有象(3)那种“线性无关”的，那么 G 就是无穷循环群 $(a_1),\cdots,(a_n)$ 的直积，下面我们用反证法来证明这事实．

假如 G 的极小生成元集中没有象(3)那种线性无关的，显然在这些关系的所有正幂中存在最小的，我们命(3)就是这样的一个关系，其中 λ_1 是最小正幂．假定

$$\lambda_i=q_i\lambda_1+\mu_i,\ 0\leqslant\mu_i<\lambda_1,\ i=2,\cdots,n.$$

那么 $b=a_1a_2^{q_2}\cdots a_n^{q_n},a_2,\cdots,a_n$ 又是 G 的生成元集，它们有关系

$$b^{\lambda_1}a_2^{\mu_2}\cdots a_n^{\mu_n}=e.$$

因为 $0\leqslant\mu_i<\lambda_1$，而 λ_1 是最小正幂，所以 $\mu_2=\cdots=\mu_n=0$．于是 $b^{\lambda_1}=e$．但 G 是纯无穷群，所以 $b=e$，因此 $a_2,\cdots,a_n$ 就成为 G 的生成元集，这与 $a_1,\cdots,a_n$ 是极小生成元集的假设不合，所以 G 的极小生成元集中有象(3)那样线性无关的，因此 G 是 $(a_i),i=1,\cdots,n$ 的直积．

再与 §4.1 定理 2 类似，假如 G 是 $(a_1),\cdots,(a_n)$ 的直积，那么 G 中任意 $n+1$ 个元都没有象(3)那样线性无关的，因此 G 的直积因子 (a_i) 的个数 n 是唯一的．又因为无穷循环群都同构，所以 G 能够唯一地分解为 n 个无穷循环群的直积．因此定理成立．

定理 6 由有穷个元生成的交换群 G 能够唯一地分解为有穷群与纯无穷群的直积.

证明 假定 H 是 G 中所有阶数是有穷的元形成的子群,即 G 的周期子群,如果子群 H 也是由有穷个元生成的. 那么 H 就是有穷群. 如果 H 是由无穷个元生成的,因为 G 中其它元都是无穷阶的不能在 H 中,所以这无穷个生成元是 G 的生成元的一部分. 这与 G 是有穷个元生成的假设矛盾. 所以 H 是由有穷个元生成的.

由 § 2.3 定理 7,$\overline{G}=G/H$ 是纯无穷群. 再 G 的生成元在 $\overline{G}$ 的象,显然就是 G 的生成元,因此 $\overline{G}$ 也是由有穷个元生成的群. 于是由定理 5,$\overline{G}$ 是无穷循环群$(\overline{a}_1),\cdots,(\overline{a}_k)$的直积:

$$\overline{G}=(\overline{a}_1)\times\cdots\times(\overline{a}_k).$$

命 $K=(a_1)\cdots(a_k)$,这里 a_i 是 $\overline{a}_i$ 在 G 中象源,因为 $\overline{a}_i$ 的阶都是无穷,所以 a_i 的阶也都是无穷,于是 K 是纯无穷群. 显然 K 是(a_1),$\cdots$,(a_k)的直积:$K=(a_1)\times\cdots\times(a_k)$. 因为如果 $a_1^{n_1}\cdots a_k^{n_k}=e$,那么 $\overline{a}_1^{n_1}\cdots\overline{a}_k^{n_k}=\overline{e}$,因此 $n_1=0,\cdots,n_k=0$. 下面我们来验证 $G=K\times H$.

首先,对于 G 中任意元 g,由 $\overline{g}\in\overline{G}$,我们有

$$\overline{g}=\overline{a}_1^{r_1}\cdots\overline{a}_k^{r_k}=\overline{a_1^{r_1}\cdots a_k^{r_k}},$$

因此

$$g=h\cdot a_1^{r_1}\cdots a_k^{r_k},h\in H.$$

即 $g=hk,h\in H,k\in K$. 再因为 H 中元的阶数都是有穷,而 K 是纯无穷群,所以 $H\cap K=E$(G 的单位元群),因此 G 是 H,K 的直积.

再假如 G 又能分解为有穷群 H' 与纯无穷群 K' 的直积,即 $G=H'\times K'$. 因为 $K'\simeq G/H'$ 是纯无穷群,所以 H' 是 G 中所有阶数是有穷的元形成的子群. 因此 $H'=H$,于是 $K\simeq K'$. 这就是说,G 分解为有穷群与纯无穷群的直积是唯一的.

于是定理得证.

根据上面三个定理容易推得下面的交换群基本定理[12].

定理 7 由有穷个元生成的交换群能够唯一地分解为循环 p 群与无穷循环群的直积.

这定理的基本内容高斯已早知道,但完备的证明是 1879 年弗罗宾纽斯和施梯克尔贝尔格尔(L. Stickelberger)首先给出的.

上面各定理中的 G,我们没有考虑它的算子集,假如算子集是域,或者是主理想环,上面的定理也都能够同样成立. 即主理想上的有穷生成模可以唯一地分解为循子模的直和域[13].

下面我们来补证 §2.3 中提出而没有给出证明的定理:对交换群拉格朗日定理的逆成立.

假定 G 是 n 元交换群,$n=p_1^{r_1}\cdots p_k^{r_k}$,$m=p_1^{s_1}\cdots p_k^{s_k}$,$s_i\leqslant r_i$,因为 $G=G_{p_1}\times\cdots\times G_{p_k}$,$G_{p_i}$ 是循环 p 群的直积,又因为对于循环群,拉格朗日定理成立,因此得知 G_{p_i} 有 $p_i^{s_i}$ 元子群,命其一为 H_i,于是

$$H=H_1\times\cdots\times H_k$$

就是元数为 m 的子群. 这就是说,如果 $m|n$,那么 G 有 m 元子群. 即当 G 是交换群时,拉格朗日定理的逆是成立的.

最后,我们还来介绍交换群的一个重要性质.

假定 G 是交换群,F' 是域 F 的乘群,假如 χ 是 G 到 F' 的同态,那么 χ 叫做 G 在 F 的**群指标**,或者简称为 G 的**群指标**. 两个群指标 χ_1,χ_2,如果对于 G 中任意元 a,有 $\chi_1(a)=\chi_2(a)$,那么 χ_1,χ_2 就相等:$\chi_1=\chi_2$. 它们的乘积 $\chi_1\chi_2$,我们规定是

$$\chi_1\chi_2(a)=\chi_1(a)\cdot\chi_2(a),$$

因此 $\chi_1\chi_2$ 又是 G 在 F 的群指标. 我们容易知道,G 在 F 的所有群指标形成可换群 G',叫做 G 在 F 的**群指标群**,或简称为 G 的**群指标群**. 这时 G' 的单位元是群指标

$$\chi_0(a)=e,e \text{ 是 } F \text{ 的单位元}.$$

下面,是有穷交换群与它的群指标群间的一个基本性质.

假定 G 是有穷交换群,$G=(a_1)\times\cdots\times(a_n)$,循环群 (a_i) 的元数是 n_i,因为 G 中任意元 a 可以写成

$$a=\prod_{i=1}^{n} a_i^{r_i}, 0\leqslant r_i < n_i,$$

所以 $\chi(a)=\prod\limits_{i=1}^{n}\chi(a_i)^{r_i}$. 再因为 $\chi(a_i)$ 是 $x^{n_i}=e$ 的零点，并且 $x^{n_i}=e$ 在 F 中的所有零点形成一个循环群 (a_i')，它的元数 m_i 是 n_i 的因数 $m_i|n_i$，所以 $\chi(a_i)=a_i'^{s_i}, 0\leqslant s_i\leqslant m_i$. 命 χ_i 是使 $\chi_i(a)=a_i'^{r_i}$ 的群指标，因而 $\chi_i(a_i)=a_i'$, $\chi_i(a_j)=e, i\neq j$. 由于

$$\chi(a)=\prod_{i=1}^{n}(a_i'^{r_i})^{s_i}=\prod_{i=1}^{n}\chi_i(a)^{s_i},$$

所以

$$\chi=\prod_{i=1}^{n}\chi_i^{s_i}.$$

也就是说，这时 G' 中任意元 χ 可以写成 χ_i 的乘积.

设 H 是 n 个无穷循环群 (b_i) 的直积，即 $H=(b_1)\times\cdots\times(b_n)$，我们命 H 中元 $\prod\limits_{i=1}^{n} b_i^{t_i}$ 与 G 中元 $\prod\limits_{i=1}^{n} a_i^{t_i}$ 对应，这对应显然是 H 到 G 上的同态，因此

$$G\simeq H/K_1,$$

这里 K_1 是 H 中所有形如 $\prod\limits_{i=1}^{n} b_i^{t_i}, t_i\equiv 0(n_i)$，的元组成的子群. 同样，我们有

$$G'\simeq H/K_2,$$

这里 K_2 是 H 中所有形如 $\prod\limits_{i=1}^{n} b_i^{t_i}, t_i\equiv 0(m_i)$，的元组成的子群. 因为 $m_i|n_i$，所以 $K_2\supseteq K_1$. 假定 K 是 H/K_1 中 K_2/K_1 在 G 的完全象源，由第一同构定理，我们有

$$G/K\simeq(H/K_1)/(K_2/K_1)\simeq H/K_2\simeq G'.$$

假如 $|G|=d$，而 F 含有 d 次本原单位根，因而 F 也含有 n_i 次本原单位根，于是 $x^{n_i}=e$ 在 F 中完全分裂，因此 $m_i=n_i$. 所以 $K_1=K_2$. 显然，这时 $K=E$，因此 $G\simeq G'$. 于是我们有

定理8　有穷交换群 G 与它在 F 的群指标群 G' 同态．假如 G 的元数是 d，而 F 含有 d 次本原单位根，那么 G 与 G' 同构．

习　题　6.5

1. 18 元交换群有几种分解？也就是说，它有几种类型？

2. 试证 6 元群只有循环群及对称群 S_3 两类．

3. 有穷交换群成为循环群的必要充分条件是群的元数为群中所有元素阶数的最小公倍．

4. 周期群是否是有穷群．

5. 试证任意有穷交换群 G 能够分解为元数是 n_i 的循环群 (a_i) 的直积，即

$$G=(a_1)\times\cdots\times(a_m),$$

并且

$$n_i\mid n_{i+1},i=1,2,\cdots,m-1.$$

6. 假定交换群 $G=\{a_1,\cdots,a_n\}$，试证

$$\sum\chi(a_i)=ne，当\ \chi=\chi_0,$$
$$=0，当\ \chi\neq\chi_0.$$

§6.6　可迁群、非迁群

这节，我们来讨论由变换形成的群，下章我们将要引用它．

我们知道克莱茵四元群

$$B_4=\{1,(12)(34),(13)(24),(14)(23)\}$$

及

$$B=\{1,(12),(34),(12)(34)\}$$

都是由 4 个文字 1，2，3，4 上的排列组成的群，前者含把 1 变为 1，2，3，4 的各个排列；但后者则否，它只含把 1 变为 1，2 的排列，不含把 1 变为 3 或 4 的排列．这是变换群的一个基本性质，一般变换群可以根据这性质来分类．

定义　假定 G 是集合 M 上变换群的子群，a 是 M 中某元，如果对于 M 中任意元 b，G 中就有使 $\sigma(a)=b$ 的变换 σ，那么 G 叫做 M 的可迁群，否则就叫做 M 的非迁群．

于是，B 是 4 个文字上的非迁群，B_4 是 4 个文字上的可迁群．n 个文字上的对称群 S_n 及交代群 A_n 显然都是可迁群．

要注意的是，在上面定义中，元 a 可以任意选取，不影响群的可迁性．这是因为，假如 G 是 M 的可迁群，$\sigma(a)=b,\tau(a)=c$，那么

$$\tau\sigma^{-1}(b)=\tau(a)=c,$$

因此，对于 M 中的任意两元 b,c，在 G 中含有把 b 变为 c 的变换．

下面是可迁群的基本性质．

假如 G 是 M 的可迁群，显然 G 中所有不使 M 中元 a 变动的变换成为一个子群 G_a，陪集 τG_a 中任意变换把 a 变为 $\tau(a)$．于是 $\tau G_a\tau^{-1}$ 不使 $\tau(a)$ 变动，因此 $\tau G_a\tau^{-1}\subseteq G_{\tau(a)}$．同样，$\tau^{-1}G_{\tau(a)}\tau$ 不使 a 变动，所以 $\tau^{-1}G_{\tau(a)}\tau\subseteq G_a$，这就是说，$G_{\tau(a)}\subseteq\tau G_a\tau^{-1}$．因此我们有

$$G_{\tau(a)}=\tau G_a\tau^{-1}.$$

再假如我们把 G_a 的陪集 τG_a 与 $\tau(a)$ 对应，这对应显然是单射．因为 G 是可迁群，所以 G 中陪集 τG_a 的个数等于 M 的元数，也就是说，G 关于 G_a 的指标 $|G:G_a|$ 等于 M 的元数 $|M|$．即 G 的元数等于 M 的元数的倍数．

可迁群又可象下面那样再分类．

假如 G 是 M 的可迁群，如果 M 能够分为一个以上没有公共元的子集 $M_1,M_2,\cdots$，并且 M_i 的元数不完全都是 1，使 G 中任意变换能够把每个 M_i 变为一个 M_j，那么 G 就叫做非原群，而 $M_1,M_2,\cdots$，叫做 G 的非原系．如果 M 不能这样划分，那么 G 就叫做本原群．

譬如对称群 S_n 是本原群，这是因为，假如它是非原群，命 $M_1=\{1,\cdots,k-1,k\}$，那么对换 $(k,k+1)$ 把 M_1 变为 $M_2=\{1,\cdots,k-1,k+1\}$，这时 $M_1\neq M_2$，而 $M_1\cap M_2=\{1,\cdots,k-1\}$，这与非原系的性质不合，所以 S_n 是本原群．同样，交代群 A_n 也是本原群，再 B_4 是非原群，而

$$M_1=\{1,2\},M_2=\{3,4\};M_1=\{1,3\},M_2=\{2,4\};$$

$$M_1=\{1,4\},M_2=\{2,3\}$$

都是它的非原系．因此我们得知一个非原群的非原系不是唯一的．

假如 G 是非原群，$M_1,M_2,\cdots$ 是它的非原系，那么 G 中含有把 M_i 中元 a_i 变为 M_j 中元 a_j 的变换，这变换显然就把 M_i 变为 M_j，所以 M_i 的元数等于 M_j 的元数，因此非原系 $M_1,M_2,\cdots$ 的各个元数都相等．假如 M 的元数是质数，那么 G 就是本原群．

定理1 假定 G 是集合 M 的可迁群，G_a 是其中不使 M 中元 a 变动的所有变换形成的子群，那么 G 是非原群的必要充分条件是 G 有适合下面关系的子群 H：

$$G\supset H\supset G_a.$$

证明 假定 G 是非原群，$M_1,M_2,\cdots$ 是它的非原系，M_1 的元数大于 1，a 是 M_1 中元，显然 G 中所有把 M_1 中元仍然变为 M_1 中元，也就是说不使 M_1 变动的变换成为一个子群，我们命它为 H．因为 H 包含 G 中所有不使元 a 变动的变换，又包含把 a 变为 M_1 中其他元的变换，所以 $H\supset G_a$．再因为 G 是可迁群，所以它包含把 a 变为 M_2 中元的变换，因此 $G\supset H$．这就是说，$G\supset H\supset G_a$．所以必要条件成立．

反过来，假如 H 是 G 的子群，并且 $G\supset H\supset G_a$，我们把 G 分为若干个 H 的陪集 τ_iH，显然集合

$$M_i=\tau_iH(a)$$

的个数不小于 2，并且每个集合都包含两个以上的元．因为 G 包含把 a 变为 M 中任意元的变换，所以 M 中任一元必在某个 M_i 中．再任意两个 M_i,M_j 没有公共元，这是因为，假如

$$\tau_i\sigma_i(a)=\tau_j\sigma_j(a),\sigma_i,\sigma_j\in H,$$

那么 $\sigma_j^{-1}\tau_j^{-1}\tau_i\sigma_i(a)=a$，因此

$$\sigma_j^{-1}\tau_j^{-1}\tau_i\sigma_i\in G_a\subset H,$$

于是 $\tau_i\in\tau_jH$，这与假设不合．因此 M 能够划分为这样的 M_i 类．又假如 ρ 是 G 中任意元，因为

$$\rho M_i=\rho\tau_i H(a)=\tau_j H(a)=M_j,$$

所以 ρ 把 M_i 变为 M_j，因此 G 是非原群，所以充分条件成立．于是定理得证．

假如 $G\supset H_1\supset G_a$，H_1 是 G 的子群，如果 $H_1(a)=H(a)$，我们容易证明 $H_1=H$. 因此适合 $G\supset H\supset G_a$ 的子群 H 的个数（a 是固定的）就是 G 的不同的非原系的个数，这样我们就可以把 G 的全部非原系找出．譬如 4 元置换群 $G=((1234))$，$G_1=((1))$，这时只有一个

$$H=\{(1),(13)(24)\}.$$

因此它的非原系只有一个（$H(1)=\{1,3\}$，$(1234)H(1)=\{2,4\}$）：

$$\{1,3\},\{2,4\}.$$

对于体，也有所谓本原的与非原的之分．假如 K 是 F 的有穷次代数体，如果 K 中不属于 F 的元都是关于 F 的本原元，那么 K 叫做**本原体**；否则就叫做**非原体**．

最后是非迁群的基本性质．

假如 G 是集合 M 的非迁群，我们可以把 M 这样来分类，先在 M 中任取一元，把 G 的各变换对于这元在 M 的所有象作为一子集，再在 M 中任取不属于这子集的一元，把这元的所有象又作为一子集，这样继续下去，我们可以把 M 划分为若干个这样没有公共元的子集．显然，对于任意子集中某一元，G 中有把它变为这集中任一元的变换，并且 G 中任意变换把任意子集中元仍然变为该子集中元．也就是说，对于这些子集来说，G 都是可迁的．这些子集我们又叫它做 G 的**可迁系**．

譬如 $\{1,2\}$，$\{3,4\}$ 就是非迁群 B 的可迁系．

要注意的是，虽然可迁群的非原系中各个子集的元数是相等的，但是非迁群的可迁系中各个子集的元数却不一定相等，譬如

$$\{1,(123),(132),(45)(123)(45),(132)(45)\}$$

是集合 $\{1,2,3,4,5\}$ 的非迁群，它的可迁系是 $\{1,2,3\}$，$\{4,5\}$.

定理 2 假定可迁群 G 的正规子群 H 是非迁群，那么 H 的

可迁系中各个子集的元数相等.

证明 假如G是关于$\{1,2,\cdots,m\}$的可迁群,

$$\{1,2,\cdots,k\}\ k<m,$$

是H的可迁系中一子集,我们命i是不属这子集的任意数. 因为G是可迁的,所以它含有把1变为i的变换. 假定$\sigma(1)$等于i,那么$\sigma(1),\sigma(2),\cdots,\sigma(k)$又是$\sigma H\sigma^{-1}=H$的可迁系中一子集. 这因为,$H$中含有把1变为$\{1,2,\cdots,k\}$中任意元的变换,因此$\sigma H\sigma^{-1}$中含有把$\sigma(1)$变为$\{\sigma(1),\sigma(2),\cdots,\sigma(k)\}$中任意元的变换. 假如$\sigma H\sigma^{-1}$中含有把$\sigma(1)$变为$\sigma(k+1)$的变换,那么$H$中就有把1变为$k+1$的变换,这与假设不合. 因此$\sigma(1),\sigma(2),\cdots,\sigma(k)$是$H$的可迁系中一子集. 因为$i$是任意数,所以$H$的可迁系中任一子集都是由$k$个数组成的,这就是说,$H$的可迁系中各个子集的元数相等,因此定理成立.

在上面的证明中,假如m是质数,因为$k|m$,那么$k=1$,于是我们得知,对于元数是质数的集合的可迁群,它的正规子群除单位元群外,都是可迁群.

习 题 6.6

1. 假如G是M的可迁群,G的元数是n,M的元数是m,试证$m|n$.

2. 假定G是$M=\{1,2,\cdots,m\}$的可迁群,G_i是G中所有不使i变动的变换形成的子群,试证$G_1,G_2,\cdots,G_m$中任意两个群共轭. 假如M中对于G_k中任意变换都不动的数字的个数是m_k,那么G_k的正规化子的元数是$g_k m_k$,这里g_k是G_k元数.

3. 假定$G=\{g_1,g_2,\cdots,g_k\}$是$\{a_1,a_2,\cdots,a_m\}$的可迁群,$H=\{h_1,h_2,\cdots,h_l\}$是$\{b_1,b_2,\cdots,b_n\}$的可迁群,试证kl个排列

$$g_ih_j,i=1,2,\cdots,k;j=1,2,\cdots,l.$$

成为$\{a_1,\cdots,a_m,b_1,\cdots,b_n\}$的非迁群,并且$\{a_1,a_2,\cdots,a_m\}$,$\{b_1,b_2,\cdots,b_n\}$是它的可迁系.

4. 试证6元群$G=((123456))$,$G_1=((1))$时的子群只有二个

$$H=\{(1),(14)(25)(36)\},H_1=\{(1),(135)(246)\}$$

因此G的非原系也只有二个，求出这二个非原系．

5. 试证对称群S_6的子群

$$H=\{(1),(145)(236),(154)(263),(12)(35)(46),\\(13)(24)(56),(16)(25)(34)\}$$

是$M=\{1,2,3,4,5,6\}$的非原群，并求出它的所有非原系．

参 考 文 献

[1] W. E. Barnes, Intrcduction to abstract algebra(1963), 89～92.

[2] Bender, H, A group theoretic proof of Burnside's p^aq^b-theorem, Math. Z. 126(1972), 327～338.

Matsuyama, H., Solvability of groups of order 2^ap^b. Osaka. J. Math. 10(1973), 375～378.

[3] Hua, Loo-Kang(华罗庚), On the multiplicative groups of a field, 科学记录，第三卷第一期(1950), 1～6.

W. R. Scott, On the multiplicative group of a division ring, Proc. Amer. Math. Soc., 8(1957), 303～305.

[4] W. Feit and J. G. Thompson, Solvability of groups of odd order, Pacific Jour. of Math. Vol. 13, No. 3(1963).

[5] M. 赫尔，群论(裘光明译), 182.

张远达，有限群构造，科学出版社(1982)，第十章

[6] I. Kaplansky, Infinite abelian groups, The University of Michigan Press Am. Arbor, 1962.

L. Fuchs, Abelian Groups, Pergamon press, New York, 1967.

R, Hirshon, On Cancellation in groups, Amer. Math. Monthly, 76 (1969)1037～1039.

——, Cancellation of Groups with maximal condition, Proc. Amer. Math. Soc. 24(1970), 401～403.

——, The Cancellation of an infinite cyclic group in direct products, Arch Math. (Basel)26(1975), 134～138.

[7] Gilner, Robert, W. Jr., The Cancellation Law for ideals in a commutative ring, Can. J. Math. 17(1965), 281～287.

[8] N. 贾柯勃逊：抽象代数学(黄缘芳译)，卷1第五章，143～144.

[9] Jacob Basshay, Topics in Riug Theory. p. 111.

[10] A. Г. 库洛什,群论(曾肯成、郝炳新译),§ 20

张远达,有限群构造,上册,149 页

J. S. Rase, A cousse On group theory, p. 54.

[11] A. П. 吉兹曼:周期群的伯恩赛德问题,数学通报 9(1963),33.

[12] E. Schenkman, The basis Theorem for finitely generated abelian groups, Amer, Math. Monthly, 67(1960), 770～771.

[13] N. Jacobson,基础代数,第一卷,第一分册,高教出版社(1987),222～223.

靳平,有限生成模唯一性的新证明,武汉大学学报 1986 年第 4 期 25～26.

第7章

伽罗瓦理论

这章介绍有穷次可离正规域的伽罗瓦理论，它在代数及代数数论上都占有重要地位. 前三节介绍基本概念及基本性质，后四节主要讨论多项式用根号解出的问题，是伽罗瓦理论的一个重要应用. 这问题是借伽罗瓦理论获得解决的，伽罗瓦理论之来也正是从这问题所引起. 很多关于域的问题可以化为域的自同构形成的群的问题来讨论，容易得到解决. 这是伽 罗瓦理论的基本思想，其重要也就在此.

这章讨论的体都是域.

§7.1 伽罗瓦群

我们知道，假定 K 是域 F 的 n 次可离域. 根据§5.7 定理 1，我们可以把 K 写成 $K=F(\alpha)$. 如果 $f(x)$ 是 $F[x]$ 中 α 适合的 n 次既约多项式，$L(\supseteq F)$ 是 $f(x)$ 的分裂域，由§5.6 定理 6，得知在 L 中，K 关于 F 的同值映射有 n 个互异的，并且不论 L 如何扩大，在同一域中，这样互异的同值映射不能多于 n 个. 假如 $f(x)$ 在 L 中的零点是 $\alpha_1(=\alpha),\alpha_2,\cdots,\alpha_n$，那么在 L 中，K 关于 F 的同值映射是把 $f(x)$ 的零点 α 仍然变为 $f(x)$ 的零点 α_k，因此，把 $F(\alpha)$ 中元 $\sum\limits_{i=0}^{n-1}a_i\alpha^i$ 变为 $\sum\limits_{i=0}^{n-1}a_i\alpha_k^i$，所以这同值映射是把 $F(\alpha)$ 变为它的共轭域 $F(\alpha_k)$，这同值映射我们用 σ_k 表示，即

$$\sigma_k(\alpha)=\alpha_k.$$

假如 $K=F(\alpha)$ 又是 F 的正规域，那么 $F(\alpha)=F(\alpha_k)$，所以 K 关于 F 的同值映射是 K 的自同构. 它不使 F 中任意元变动. 显然，K 的这样自同构的逆以及任意两个这样自同构的积仍然是这样的自同构. 因此，所有这样不使 F 中任意元变动的 K 的自同构成为一个群，这群叫做 K 关于 F 的**伽罗瓦群**，或者叫做 K 关于 F 的**群**，我们用 G 来表示. 这就是说，正规域 K 关于 F 的伽罗瓦群 G 是所有不使 F 中任意元变动的 K 的自同构组成的群. §5.5 中所以叫 K 做 F 的伽罗瓦域，其原因就是它的群 G 叫做伽罗瓦群. 由 §5.6 定理 8，我们得知 $|G|=(K:F)=n$，于是 K 关于 F 的伽罗瓦群

$$G=\{\sigma_1,\cdots,\sigma_n\}.$$

上面，我们介绍 K 关于 F 的同值映射是先把 K 写成 F 的单扩张，因此引用了 K 的本原元，但这引用只是为了方便，并不是非如此不可. 假定 K 是由 F 陆续添加 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 形成的扩张域，即 $K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，那么，在 K 的适当扩张域 L 中，K 关于 F 的同值映射可以这样来求得，先求出 $F(\alpha_1)$ 关于 F 的同值映射，这些同值映射都把 α_1 变成它的共轭元，然后将这些同值映射延长成为 $F(\alpha_1,\alpha_2)$ 关于 F 的同值映射，就得到在 L 中 $F(\alpha_1,\alpha_2)$ 关于 F 的所有同值映射. 这样继续下去，最后将 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$ 关于 F 的所有同值映射延长，就得到在 L 中 K 关于 F 的所有同值映射.

我们知道 G 中任意元不使 F 中任意元变动，它的逆也成立. 这就是

定理 1 假定 G 是 K 关于 F 的伽罗瓦群，那么 K 中关于 G 的任意元不变动的元都在 F 中.

证明 因为 K 中任意元 α 适合的 $F[x]$ 中既约多项式的次数等于 α 关于 F 互异共轭元的个数. 如果这个数等于 1，那么 α 就是 F 中元了. 假定 α' 是 α 在 K 中关于 F 的任意共轭元，因为 $F(\alpha)$，$F(\alpha')$ 关于 F 同值，由 §5.5 定理 3，我们可以把它延长成为 K 的自同构. 因此 G 中有把 α 变为 α' 的元. 现在 G 中所有元都不使 α 变

动，所以 $\alpha'=\alpha$，这就是说 α 的共轭元只有它自身，即 α 的共轭元的个数等于1，因此定理得证.

于是 K 中元在 F 中的必要充分条件是：它的伽罗瓦群 G 中任意元不使它变动，这是伽罗瓦群一个最基本的性质. 再由上面的证明，我们又得知，假如 α,β 是 K 中关于 F 的共轭元，那么 G 中有把 α 变为 β 的元.

域 F 的有穷次可离正规域，当它关于 F 的伽罗瓦群是阿贝耳群时，就叫做 F 的**阿贝耳域**，是循环群时，就叫做 F 的**循环域**.

下面我们给出几个伽罗瓦群的例.

假定 Q 是有理数域，

$$K=Q(\omega,\sqrt[3]{2}),\omega=\frac{1}{2}(-1+i\sqrt{3}),$$

是 Q 的正规域，显然 $\omega+\sqrt[3]{2}$ 是它的本原元，但我们不把 K 写成单扩张，因为这样反而麻烦. 因为 K 中元是系数是 Q 中元的 $\sqrt[3]{2}$，ω 的多项式，又因为 $\sqrt[3]{2}$，ω 分别是 Q 中既约多项式

$$x^3-2=(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2}),$$

$$x^2+x+1=(x-\omega)(x-\omega^2)$$

的零点，而 K 关于 Q 的伽罗瓦群 G 中元把它们的零点仍然变为它们的零点，所以 $\sqrt[3]{2}$ 的象只能有3个，ω 的象只能有2个. 但是 $\omega\overline{\in}F(\sqrt[3]{2})$，所以合并它们就得到下面6个不使 Q 中元变动的 K 的自同构：

	$\sigma_0=1$	σ_1	σ_2	σ_3	σ_4	σ_5
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$
ω	ω	ω	ω	ω^2	ω^2	ω^2

因为 $(K:Q)=6$，所以这6个自同构就是 G 的全部元. 再由计算容易得知

$$\sigma_2=\sigma_1^2,\sigma_4=\sigma_1\sigma_3,\sigma_5=\sigma_2\sigma_3=\sigma_1^2\sigma_3.$$

因此 $$G=\{1,\sigma_1,\sigma_1^2,\sigma_3,\sigma_1\sigma_3,\sigma_1^2\sigma_3\}$$

即 $$G=\langle\sigma_1,\sigma_3\rangle,\sigma_1^3=1=\sigma_3^2,\sigma_3\sigma_1\sigma_3=\sigma_1^2,\sigma_3\sigma_1^2\sigma_3=\sigma_1.$$

显然 G 与对称群 S_3 同构，即 $G\simeq S_3$. 这就是说，K 关于 Q 的伽罗瓦群是 S_3.

再假定 $K=Q(\xi)$，ξ 是 n 次本原单位根. 显然 K 是 Q 的正规域. 我们知道，ξ^{n_k}是 n 次本原单位根的必要充分条件是 n,n_k 互质，即$(n,n_k)=1$. 假如 $n_1,\cdots,n_{\varphi(n)}$是模 n 的简化剩余系[1]，于是我们有分圆多项式

$$\Phi_n(x)=\prod_{i=1}^{\varphi(n)}(x-\xi^{n_i}),$$

它是$Q[x]$中 $\varphi(n)$次既约多项式，假设 σ_i 是 K 关于 Q 的伽罗瓦群 G 中的任意元，因为 σ_i 把 $\Phi_n(x)$的零点仍然变为 $\Phi_n(x)$的零点，设 $\sigma_i(\xi)=\xi^{n_i}$，因此

$$\sigma_i\sigma_j(\xi)=\sigma_i(\xi^{n_j})=(\sigma_i(\xi))^{n_j}=(\xi^{n_i})^{n_j}=\xi^{n_in_j}=\xi^{n_k},$$

式中 $n_in_j\equiv n_k(n)$. 因为$(n_i,n)=1,(n_j,n)=1$，所以$(n_in_j,n)=1$. 因此 $\sigma_i\sigma_j=\sigma_k$. 假如命 σ_i 与 n_i 对应，即 $\sigma_i\to n_i$，那么，这对应就是 $G=\{\sigma_1,\cdots,\sigma_{\varphi(n)}\}$与乘群$\{n_1,\cdots,n_{\varphi(n)}\}$的同构，因此 G 是交换群[2]. 所以 K 是 Q 的阿贝耳域.

假如 n 是质数，那么 n 的简化剩余系对乘法成为一个循环群(§5.8)，因此 G 是 $n-1$ 元循环群，所以这时 K 就是 Q 的循环域.

此外，我们还有

定理 2 假定 F 含有 n 次本原单位根，$K=F(\alpha)$，这里 α 是纯多项式 $f(x)=x^n-a,a\in F$ 的零点，也就是说，α 是 F 中某元的 n 次根，那么 K 是 F 的循环域.

证明 显然 K 是 F 的正规域. 假定 ξ 是 F 中 n 次本原单位根. 那么 $\alpha,\xi\alpha,\cdots,\xi^{n-1}\alpha$ 是 K 中 $f(x)$的零点，如果 $f(x)$是既约的，那么 K 关于 F 的次数是 n，因此 K 关于 F 的伽罗瓦群 G 与 n 次单位根形成的循环群同构. 所以 G 是 n 元循环群.

如果 $f(x)$ 是可约的，那么 K 关于 F 的伽罗瓦群 G 中元 σ_i 把 $f(x)$ 的零点 α 变为某零点 $\xi^{n_i}\alpha$，即 $\sigma_i(\alpha)=\xi^{n_i}\alpha$，因为

$$\sigma_i\sigma_j(\alpha)=\sigma_i(\xi^{n_j}\alpha)=\xi^{n_j}\sigma_i(\alpha)=\xi^{n_i+n_j}\alpha=\xi^{n_k}\alpha$$

式中 $n_i+n_j\equiv n_k(n)$. 我们命 σ_i 与 ξ^{n_i} 对应，即 $\sigma_i\to\xi^{n_i}$. 显然，这对应是 G 与由某些 n 次单位根组成的群的同构. 由 § 5.8 定理 5，n 次单位根组成的群是循环群，因此它的子群也是循环群. 所以 G 是循环群，于是 K 是 F 的循环域，定理证毕.

定理 3 有穷域是它的质域的循环域.

证明 假定 $K=GF(p^n)$，F 是它的质域. 由 § 5.8，K 是 F 的正规域. 对于 K 中任意元 α，我们命 α^p 与它对应，即 $\alpha\to\alpha^p$. 因为由 § 5.8，K 中任意元 $\alpha=\alpha^{p^n}$，所以 K 中任意元 α 可以写成 $(\alpha^{p^{n-1}})^p$，我们容易得知 $\alpha\to\alpha^p$ 是 K 的自同构. 当 $\alpha\in F$ 时，$\alpha^p=\alpha$，因此这同构不使 F 中任意元变动，所以它是伽罗瓦群 G 中元，我们用记号 σ 表示，即 $\sigma(\alpha)=\alpha^p$. 于是 $\sigma,\sigma^2,\cdots,\sigma^n=1$ 都是 G 中元. 由 § 5.8，K 中有阶数为 p^n-1 的元，因此这 n 个自同构互异，但 $(K:F)=n$，所以 G 的元数是 n. 于是 $G=\{\sigma,\sigma^2,\cdots,\sigma^n=1\}$，即 G 是 n 元循环群，所以 K 是它的质体的循环域. 定理证毕.

定理 4 假定 L 是 K、F 的中间体，即 $K\supseteq L\supseteq F$，G 是 K 关于 F 的伽罗瓦群，H 是 K 关于 L 的伽罗瓦群，那么 H 是 G 的子群，并且

$$G=\sigma_1H\cup\sigma_2H\cup\cdots\cup\sigma_nH$$

这里 σ_i 是 G 中所有这样的映射，σ_i 不使 K-L 中任意元变动，并且 σ_i 是 L 关于 F 的同值，即 σ_i 是 G 中某元产生的 L 关于 F 的同值映射，n 是 G 中所有产生 L 关于 F 互异同值映射的个数.

证明 因为 K 的自同构不使 L 中元动的，当然也不使 F 中元动，所以 H 是 G 的子群. 再则我们易知，G 中任意元 σ 可以看成 H 中一元 τ 与某 σ_i 的乘积 $\sigma_i\tau$，因此 σ 在陪集 σ_iH 中：$\sigma\in\sigma_iH$，如果 $\sigma_iH=\sigma_jH$ 的话，那么 $\sigma_i=\sigma_j\tau$，$\tau\in H$. 于是对于 L 中的任意元 β，我们有

$$\sigma_i(\beta)=\sigma_j\tau(\beta)=\sigma_j(\beta),$$

因此 $\sigma_i=\sigma_j$. 定理成立.

求伽罗瓦群利用上定理先求出它的子群有时比较方便.

譬如,前例求 $K=Q(\omega,\sqrt[3]{2})$ 关于 Q 的伽罗瓦群,我们先求出 K 关于 $Q(\sqrt[3]{2})$ 的伽罗瓦群 H,显然 H 只有两个映射,一个是恒等映射 I,另一个是 $\tau: i\to -i$,即

$$\tau(\sqrt[3]{2})=\sqrt[3]{2},\tau(i)=-i$$

所以 $H=\{1,\tau\}$. 再因为 x^3-2 在 Q 中是既约,所以 $Q(\sqrt[3]{2})$ 关于 Q 的互异同值映射有 3 个,设 σ 是这样的一个

$$\sigma(\sqrt[3]{2})=\omega\sqrt[3]{2},\sigma(\omega)=\omega$$

因为

$$\sigma^2(\sqrt[3]{2})=\sigma(\omega\sqrt[3]{2})=\sigma(\omega)\sigma(\sqrt[3]{2})=\omega^2\sqrt[3]{2},$$

$$\sigma^3(\sqrt[3]{2})=\sqrt[3]{2}$$

所以 $\sigma^3=1$,于是

$$G=H\cup\sigma H\cup\sigma^2H=\{1,\tau,\sigma,\sigma\tau,\sigma^2,\sigma^2\tau\}$$

这结果与前面得到的一致.

讨论过 K 关于 F 的伽罗瓦群之后,我们将介绍多项式 $f(x)$ 的伽罗瓦群.

假如 $f(x)$ 是 F 的 n 次可离多项式,$\alpha_1,\cdots,\alpha_n$ 是它在同一分裂体中零点,那么 $K=F(\alpha_1,\cdots,\alpha_n)$ 是 F 的有穷次可离正规域,K 关于 F 的伽罗瓦群 G 又叫做 $f(x)$ 的**伽罗瓦群**. 这时如果 $(K:F)=m$, $G=\{\sigma_0=1,\sigma_1,\cdots,\sigma_{m-1}\}$,显然 $\sigma_i(\alpha_1),\cdots,\sigma_i(\alpha_n)$ 都是 $f(x)$ 的零点. 又因 σ_i 是 K 关于 F 的同值映射,且 $\alpha_1,\cdots,\alpha_n$ 互异,故 $\sigma_i(\alpha_1),\cdots,\sigma_i(\alpha_n)$ 也互异,因此 $\sigma_i(\alpha_1),\cdots,\sigma_i(\alpha_n)$,是 $\alpha_1,\cdots,\alpha_n$ 的一个排列. 于是对于 σ_i,我们有排列

$$s_i=\begin{pmatrix}\alpha_1 & \cdots & \alpha_n\\ \sigma_i(\alpha_1) & \cdots & \sigma_i(\alpha_n)\end{pmatrix}.$$

假如 $s_i=s_j$,那么 $\sigma_i(\alpha_1)=\sigma_j(\alpha_1),\cdots,\sigma_i(\alpha_n)=\sigma_j(\alpha_n)$. 因为 K 中任意

元 α 能够用系数是 F 中元的 $\alpha_1,\cdots,\alpha_n$ 的多项式表出，所以 $\sigma_i(\alpha)=\sigma_j(\alpha)$，这与 $\sigma_i\neq\sigma_j$ 的假设不合，于是 m 个排列 $s_0,s_1,\cdots,s_{m-1}$ 互异. 再因为

$$s_is_j=\begin{pmatrix}\alpha_1 & \cdots & \alpha_n\\ \sigma_i\sigma_j(\alpha_1) & \cdots & \sigma_i\sigma_j(\alpha_n)\end{pmatrix}$$

因此，如果我们命 σ_i 与 s_i 对应，就是 $\sigma_i\to s_i$，那么这个对应就是 G 到 $\{s_0,s_1,\cdots,s_{m-1}\}$ 上的同构，所以 G 与 $\alpha_1,\cdots,\alpha_n$ 上对称群 S_n 的子群同构，于是我们有

定理 5 n 次可离多项式 $f(x)$ 的伽罗瓦群是 $f(x)$ 的 n 个零点上对称群 S_n 的子群.

同前面类似，一个可离多项式当它的伽罗瓦群是阿贝耳群时，叫做**阿贝耳式**，是循环群时，叫做**循环式**.

譬如 Q 是有理数域，$f(x)=x^3-3x-1$，根据 § 5.5 习题 6，我们容易验证 $f(x)$ 是 Q 的正规式，如果 K 是它的分裂域，那么 $(K:Q)=3$. 因此 $f(x)$ 的伽罗瓦群 G 是 3 元循环群，但 S^3 中 3 元子群只有 A_3，所以 $G=A_3$. 同样，我们也不难证明 $f(x)=x^3-9x+2$ 不是 Q 的正规式，因此它的分裂域关于 Q 的次数是 $3\cdot 2=6$，于是 $f(x)$ 的伽罗瓦群 G 是 6 元群，所以 $G=S_3$[3].

下面是关于可离多项式的伽罗瓦群的一个常用定理.

定理 6 假定 $f(x)$ 是 F 的可离多项式，那么它的伽罗瓦群 G 是 $f(x)$ 零点的可迁群的必要充分条件为 $f(x)$ 是既约式.

证明 假如 $f(x)$ 是既约式，$\alpha_1,\cdots,\alpha_n$ 是它的零点，因为 $F(\alpha_1)\simeq F(\alpha_i)$，由 § 5.5 定理 3，这同构延长就成为 G 中元，这就是说，G 中有把 α_1 变为任意 α_i 的元，因此 G 是 $\{\alpha_1,\cdots,\alpha_n\}$ 的可迁群.

假如 $f(x)$ 是可约式，$f_1(x)$，$f_2(x)$ 是 $f(x)$ 的两个既约因式，α_1 是 $f_1(x)$ 的零点，α_2 是 $f_2(x)$ 的零点，因为 G 中元把 $f(x)$ 的零点仍然变为 $f_1(x)$ 的零点，所以 G 中没有把 α_1 变为 α_2 的元，因此 G 是 $\{\alpha_1,\cdots,\alpha_n\}$ 的非迁群.

于是定理得证.

譬如，在前面的例中，$f(x)=(x^2+x+1)(x^3-2)$的分裂域$K=Q(\omega,\sqrt[3]{2})$，所以$f(x)$的伽罗瓦群

$$G=\{1,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5\},$$

假如把$f(x)$的零点$\omega,\omega^2,\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$分别用1,2,3,4,5表示，那么

$$1=(1),\sigma_1=(3\ 4\ 5),\sigma_2=(3\ 5\ 4),$$

$$\sigma_3=(1\ 2)(4\ 5),\sigma_4=(1\ 2)(3\ 4),\sigma_5=(1\ 2)(3\ 5)$$

显然G是非迁群.

要注意的是在前例中，G是3个文字的可迁群，但在这里G是5个文字的非迁群，两者的对象不同.

习 题 7.1

1. 试证3次既约多项式的伽罗瓦群是对称群或是交代群.

2. 试证$F[x]$中多项式$f(x)$的伽罗瓦群全由偶排列组成的必要充分条件是$f(x)$的判别式的平方根在F中.

3. 假设$K=Q(\sqrt{2},i)$，Q是有理数域，试求K关于Q的伽罗瓦群及它的群表.

4. 假定$K=F(\alpha)$关于F的伽罗瓦群$G=\{\sigma_1,\cdots,\sigma_n\}$，那么$\alpha$是$F[x]$中既约多项式$f(x)=(x-\sigma_1(\alpha))\cdots(x-\sigma_n(\alpha))$的零点.

5. 试求下列各多项式关于有理数域的伽罗瓦群：

$$x^3-2,x^3+2x+1,x^4-10x^2+1.$$

6. 试证x^4-5x^2+6与x^4-10x^2+1的分裂域都是

$$K=Q(\sqrt{2},\sqrt{3}),$$

但前者的伽罗瓦群是非迁群而后者的则是可迁群.

7. 假定域F含有质数p次本原单位根，试证$x^p-a,a\in F$，在$F[x]$中或是既约，或是完全分裂为一次因式的乘积.

8. 假定域F不含质数p次本原单位根，试证$x^p-a,a\in F$，在$F[x]$中或是既约，或是$x^p-a=x^p-\alpha^p=(x-\alpha)(x^{p-1}+\alpha x^{p-2}+\cdots+\alpha^{p-1})$，这里

$$a=\alpha^p,\alpha\in F.$$

§7.2 伽罗瓦理论的基本定理

这节讨论K,F的中间体与K关于F的伽罗瓦群G的子群间的关系,它是伽罗瓦理论的基础.

假如G_1是G的子群,那么K中所有对于G_1中任意元不变动的元成为K的子域,这是因为,如果

$$\sigma(\alpha_i)=\alpha_i,\sigma(\alpha_j)=\alpha_j,\sigma\in G_1,\alpha_i,\alpha_j\in K,$$

那就有

$$\sigma(\alpha_i-\alpha_j)=\alpha_i-\alpha_j,\sigma(\alpha_i\alpha_j^{-1})=\alpha_i\alpha_j^{-1}.$$

这子域我们叫做G_1**所属的域**,用$K(G_1)$表示.因此F是G所属的域,K是单位元群E所属的域,即

$$F=K(G),K=K(E).$$

同样,假如K_1是K,F的中间体,那么G中所有不使K_1中任意元变动的元成为G的子群,这是因为,如果

$$\sigma_i(\alpha)=\alpha,\sigma_j(\alpha)=\alpha,\alpha\in K_1,\sigma_i,\sigma_j\in G,$$

那就有

$$\sigma_i\sigma_j(\alpha)=\alpha.$$

这子群,我们叫做K_1**所属的群**,用$G(K_1)$表示.因此E是K所属的群,G是F所属的群,即

$$E=G(K),G=G(F).$$

由上面的等式,我们得知

$$K(G(F))=F,G(K(E))=E.$$

把F换成K,把E换成G,上面等式也同样成立.但对于任意G_1,K_1,根据定义,我们只有

$$K(G(K_1))\supseteq K_1,G(K(G_1))\supseteq G_1,$$

假如把G_1与它所属的域$K(G_1)$对应,把K_1与它所属的群$G(K_1)$对应,那么根据上面等式,F与G一一对应,E与K也一一对应.如果上两个不等式都是等式,那么K_1与$G(K_1)$一一对应,G_1与K

(G_1)一一对应. 下面的定理就将解答这个问题, 它是**伽罗瓦理论的基本定理.**

定理1　假如K是F的有穷次可离正规域, G是K关于F的伽罗瓦群, 那么

1°　K、F的中间体K_1是$G(K_1)$所属的域, 即

$$K(G(K_1))=K_1;$$

2°　G的子群G_1是$K(G_1)$所属的群, 即

$$G(K(G_1))=G_1;$$

3°　$G(K_1)$的元数等于$(K:K_1)$, $G(K_1)$在G的指标等于$(K_1:F)$.

这定理的含义, 我们可以用下面的图式来表示:

$$\begin{array}{ccccc} & & n=kh & & \\ G & \supseteq & G_1 & \supseteq & E \\ & k & & h & \\ \updownarrow & & \updownarrow & & \updownarrow \\ F & \subsetneq & K_1 & \subseteq & K \end{array}$$

这里G_1是K_1所属的群, K_1是G_1所属的域.

$$n=\begin{cases}|G:E|=|G|,\\ (K:F);\end{cases}\quad k=\begin{cases}|G:G_1|,\\ (K_1:F);\end{cases}\quad h=\begin{cases}|G_1:E|=|G_1|,\\ (K:K_1).\end{cases}$$

证明　首先, 由§5.5定理7我们得知K是K_1的正规域. 故由定义知$G(K_1)$是K关于K_1的伽罗瓦群, 所以$K(G(K_1))\supseteq K_1$. 再由§7.1定理1, K中对于$G(K_1)$中任意元不变动的元都在K_1中, 也就是说, $K(G(K_1))\subseteq K_1$, 所以

$$K(G(K_1))=K_1,$$

因此1°成立.

其次, 假如$G_1=\{\sigma_1,\cdots,\sigma_h\}$, 因为$G(K(G_1))\supseteq G_1$, 如果我们能够证明$G(K(G_1))$的元数不大于$h$, 那么$G(K(G_1))=G_1$, 2°就告成立. 因为$G(K(G_1))$是$K$关于$K(G_1)$的伽罗瓦群, 所以我们只要证明$(K:K(G_1))\leqslant h$就行了. 现在假设$K=F(\alpha)$, 因为多项式

$$f(x)=(x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\cdots(x-\sigma_h(\alpha))$$

的系数是$\sigma_1(\alpha),\cdots,\sigma_h(\alpha)$的初等对称多项式，所以它对于任意$\sigma_i$都不变动，因此它们是$K(G_1)$中的元. 再$\alpha$是$f(x)$的零点，所以$\alpha$关于$K(G_1)$的次数不大于$h$，但$K=K(G_1)(\alpha)$，于是$(K:K(G_1))\leqslant h$，因此2°成立.

最后，因为$G(K_1)$是K关于K_1的伽罗瓦群，所以$|G(K_1)|=(K:K_1)$. 再假如

$$|G|=n,|G(K_1)|=h,|G:G(K_1)|=j$$

那么，我们就有$n=hj$，但

$$(K:F)=n,(K:K_1)=h,(K:F)=(K:K_1)(K_1:F),$$

所以$(K_1:F)=j$，因此3°成立.

于是定理得证.

我们知道$G(K_1)$是K关于K_1的伽罗瓦群，由上定理中2°又得知G_1是K关于$K(G_1)$的伽罗瓦群. 上定理是根据这个关系建立了K、F的中间体与G的子群间一一对应的关系，这是伽罗瓦理论中最基本的一个性质，它已经在多方面得到了推广.

1928年克努尔把上定理推广到次数是无穷的代数扩张域，1940年贾柯勃逊推广到一般域，1945年又推广到不是可离又不是正规的域. 1951年中山正(1912～1964)已推广到满足极小条件的环[4]. 他们对子群都要作适当限制，中间体与子群一一对应才能成立.

作为定理1的一个应用，下面我们给出§5.7定理3一个较简单的证明.

假定$K=F(\alpha)$是F的可离单扩张域，那么K、F的中间体只有有穷个. 这是因为，假如L是包含K的F有穷次可离正规域，由于L关于F的伽罗瓦群是有穷群，所以它的子群只有有穷个. 于是，由上面的主要定理得知，L、F的中间体也只有有穷个，因此K、F的中间体只有有穷个. 反过来，假如K是F的可离域，如果K、F的中间体只有有穷个，那么K关于F是有穷次，因为不如此，K、F的中间体就有无穷多个，所以K是F的单扩张域.

上面是讨论 $K(G_1)$ 与 $G(K_1)$ 的关系，现在我们来讨论，假如 K_1 已知，$G(K_1)$ 如何去求？又假如 G_1 已知，$K(G_1)$ 又如何求？

假定 $K_1=F(\beta_1,\cdots,\beta_m)$，因为 $K=F(\alpha)$，所以 β_i 是 α 的多项式．假定 G 中元 σ 把 α 变为 α_k，如果我们在表示 β_i 的 α 的多项式中把 α 换成 α_k，仍然是这个多项式，那么 σ 就不使 β_i 变动．G 中不使 $\beta_1,\cdots,\beta_m$ 变动的元也不使 K_1 中任意元变动，因此所有这些元组成的子群就是 $G(K_1)$．

再假定 $G_1=\{\sigma_1,\cdots,\sigma_m\}$，那么 K 中所有对 $\sigma_1,\cdots,\sigma_m$ 不变动的元组成的子体就是所求的 $K(G_1)$．我们也可这样来求 $K(G_1)$，由前面得知多项式

$$(x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\cdots(x-\sigma_m(\alpha))$$

的系数都在 $K(G_1)$ 中，因此把这些系数添加于 F 所得到的体 $K'\subseteq K(G_1)$，并且 $(K:K')\leqslant m$，由§4.1定理4，$(K(G_1):K')=1$，因此 $K'=K(G_1)$．这就是说，把 $\sigma_1(\alpha),\cdots,\sigma_m(\alpha)$ 的初等对称多项式添加于 F 得到的体就是所求的 $K(G_1)$．

例如在§7.1中，$K=Q(\omega,\sqrt[3]{2})$ 关于 Q 的伽罗瓦群

$$G=\{1,\sigma,\sigma^2,\tau,\sigma\tau,\sigma^2\tau\}.$$

显然它有一个3元子群 $G_1=\{1,\sigma,\sigma^2\}$，三个2元子群

$$G_2=\{1,\tau\},G_3=\{1,\sigma\tau\},G_4=\{1,\sigma^2\tau\}.$$

由计算我们容易得知，与它们对应的子体分别为

$$K_1=Q(\omega),\quad K_2=Q(\sqrt[3]{2}),$$

$$K_3=Q(\omega^2\sqrt[3]{2}),K_4=Q(\omega\sqrt[3]{2}).$$

譬如由 $K_3=Q(\omega^2\sqrt[3]{2})$，因为

$$\sigma(\omega^2\sqrt[3]{2})=\sqrt[3]{2},\sigma^2(\omega^2\sqrt[3]{2})=\omega\sqrt[3]{2},\tau(\omega^2\sqrt[3]{2})=\omega\sqrt[3]{2},$$

$$\sigma\tau(\omega^2\sqrt[3]{2})=\omega^2\sqrt[3]{2},\sigma^2\tau(\omega^2\sqrt[3]{2})=\sqrt[3]{2},$$

所以 $G(K_3)=\{1,\sigma\tau\}$，又由 $G_3=\{1,\sigma\tau\}$，因为 K 中的任意元都可以写成下面的形状：

$$a=a_1+a_2\omega+a_3\omega^2+{}_4\sqrt[3]{2}+a_5\omega\sqrt[3]{2}+a_6\omega^2\sqrt[3]{2},$$

于是

$$\sigma\tau(\alpha)=a_1+a_2\omega^2+a_3\omega+a_4\omega\sqrt[3]{2}+a_5\sqrt[3]{2}+a_6\omega^2\sqrt[3]{2},$$

但 $\sigma\tau(\alpha)=\alpha$ 的必要充分条件是

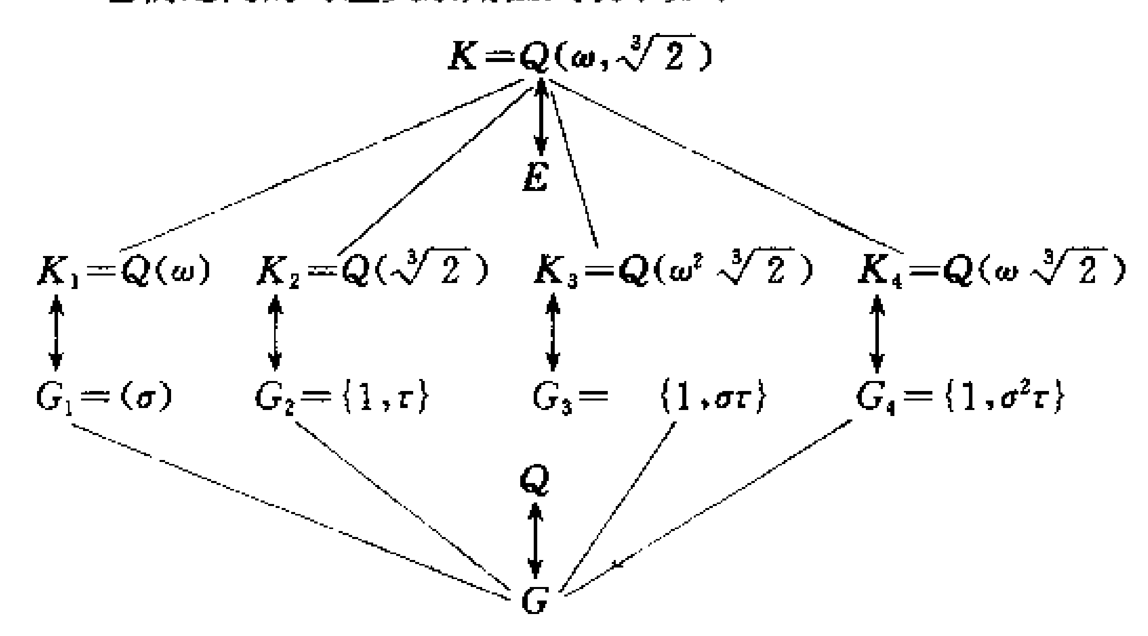
$$a_2=a_3, a_4=a_5.$$

因此

$$\begin{aligned}\alpha&=a_1+a_2(\omega+\omega^2)+a_4(\sqrt[3]{2}+\omega\sqrt[3]{2})+a_6\omega^2\sqrt[3]{2},\\&=a_1-a_2+a_4\omega^2\sqrt[3]{2}+a_6\omega^2\sqrt[3]{2}\\&=a+b\omega^2\sqrt[3]{2}, a,b\in Q\end{aligned}$$

即 $\alpha\in Q(\omega^2\sqrt[3]{2})$，所以 $K(G_3)=Q(\omega^2\sqrt[3]{2})$.

它们之间的对应关系用图式表示如下：



假如 K_1,K_2 是 K,F 的中间体，G 是 K 关于 F 的伽罗瓦群，G_1,G_2 分别是 K 关于 K_1,K_2 的伽罗瓦群，即分别是 K_1,K_2 所属的群，它们之间还有下面一些重要性质.

定理 2 假如 $K_1\supset K_2$，那么 $G_1\subset G_2$；反过来，假如 $G_1\subset G_2$，那么 $K_1\supset K_2$.

证明 假如 $K_1\supset K_2$，因为 K 的自同构如果不使 K_1 中任意元变动，显然也不使 K_2 中任意元变动，所以 $G_1\subseteq G_2$. 如果 $G_1=G_2$，那么 $K_1=K_2$，这与假设不合，因此 $G_1\subset G_2$.

再假如 $G_1 \subset G_2$，显然 $K_1 \supseteq K_2$. 如果 $K_1 = K_2$，那么 $G_1 = G_2$，这与假设不合，因此 $K_1 \supset K_2$. 所以定理得证.

我们知道，假如 G 中有元把 K_1 变成 K_2，那么 K_1, K_2 关于 F 同值. 因此 K_1, K_2 关于 F 共轭(§5.3). 反过来，假定 K_1, K_2 关于 F 共轭，也就是说 K_1, K_2 关于 F 同值，由§5.5 定理 2，我们不难得知这同值可以延长成为 K 的自同构，所以 G 中有元把 K_1 变为 K_2. 于是，K_1, K_2 关于 F 是共轭体的必要充分条件是 G 中有元把 K_1 变为 K_2. 再由§5.5 定理 6，我们又得知，中间体 K_1 是 F 的正规域的必要充分条件是 G 中任意元不使 K_1 自身变动.

定理 3 假如 K_1, K_2 关于 F 共轭，那么 G_1, G_2 共轭；反过来，假如 G_1, G_2 共轭，那么 K_1, K_2 关于 F 共轭.

证明 假如 K_1, K_2 关于 F 共轭，我们命 $\sigma(K_1) = K_2$，那么

$$\sigma G_1 \sigma^{-1}(K_2) = \sigma G_1(K_1) = \sigma(K_1) = K_2.$$

因此 $\sigma G_1 \sigma^{-1} \subseteq G_2$，同样因为 $\sigma^{-1}(K_2) = K_1$，我们有 $\sigma^{-1} G_2 \sigma \subseteq G_1$，因此 $G_2 \subseteq \sigma G_1 \sigma^{-1}$，所以 $\sigma G_1 \sigma^{-1} = G_2$.

再假定 $\sigma G_1 \sigma^{-1} = G_2$，那么

$$G_2(\sigma(K_1)) = \sigma G_1(K_1) = \sigma(K_1).$$

因此 $\sigma(K_1) \subseteq K_2$. 又因为 $G_1 = \sigma^{-1} G_2 \sigma$，所以 $\sigma^{-1}(K_2) \subseteq K_1$，即 $K_2 \subseteq \sigma(K_1)$，因此 $\sigma(K_1) = K_2$

定理证毕.

假定 K_1 与它的共轭体一致，那么 G_1 就与它的共轭群一致，因此，我们得到下面中间体是正规域的必要充分条件.

定理 4 K_1 是 F 的正规域的必要充分条件为 G_1 是 G 的正规子群.

此外，在 K 与 G 之间还有很多类似的性质，譬如 K 是可解域时，G 就是可解群；反过来 G 是可解群时，K 就是可解域.

再假如我们已经知道 K 关于 F 的伽罗瓦群，那么，我们不仅可以知道 K 关于任意中间体 K_1 的伽罗瓦群，由下面定理，我们还可以知道 K_1 关于 F 的伽罗瓦群.

定理5 假如 K_1 是 F 的正规域，那么 K_1 关于 F 的伽罗瓦群 $G'\simeq G/G_1$.

证明 因为 K_1 是 F 的正规域，所以 G 中任意元 σ 产生 G' 中一元 σ'. 由§5.5定理2，我们又得知，G' 中任意元可以延长成为 G 中元，因此，假如命 σ' 与 σ 对应，即 $\sigma\to\sigma'$，这对应显然就是 G 到 G' 上的同态. 但这同态核是 G_1，由§2.5定理5，即得 $G'\simeq G/G_1$，因此定理成立.

习 题 7.2

1. 假设 G 是 K 关于 F 的伽罗瓦群，G_1,G_2 是 G 的子群，试证 (G_1,G_2) 所属的域是 $K(G_1)\cap K(G_2)$，$G_1\cap G_2$ 所属的域是 $F(K(G_1),K(G_2))$.

2. 假如 G 是 K 关于 F 的伽罗瓦群，K_1,K_2 是 K,F 的中间体，试证 $F(K_1,K_2)$ 所属的群是 $G(K_1)\cap G(K_2)$，$K_1\cap K_2$ 所属的群是

$$(G(K_1),G(K_2)).$$

3. 假如 K 是 F 的扩张域，$F(\alpha)$ 是 F 的正规域，试证 $K(\alpha)$ 关于 K 的伽罗瓦群与 $F(\alpha)$ 关于 F 的伽罗瓦群一致的必要充分条件是

$$F(\alpha)\cap K=F.$$

4. 假如 K 是关于 F 的阿贝耳域，试证 K,F 的任意中间体是 F 的正规域，并且又是关于 F 的阿贝耳域.

5. 假如 K 是 F 的正规域，$K\supseteq L\supseteq F$，F' 是 K 中包含 L 的最小的 F 的正规域，试证 F' 所属的群是 L 所属的群与它的共轭群的交集.

6. 假如 Q 是有理数域，$K=Q(i,\sqrt[4]{2})$，求 K 关于 Q 的伽罗瓦群，并求它的子群所属的 K 的子域.

7. 假定 K 是关于 F 的有穷次不可离正规域，它的特征数是 p，L 是 K 中 F 的最大可离域，$(L:F)=n_0$，那么 K 的所有不使 F 中的任意元变动的自同构组成的群 G，叫做 K 关于 F 的伽罗瓦群，试证：

1) G 的元数等于 n_0，即 G 的元数等于 K 关于 F 的缩减次数.

2) G 是 L 关于 F 的伽罗瓦群.

3) 假定 K_1 是 K,F 的中间体，那么 $G(K_1)=G(L_1)$，这里 L_1 是 K_1 中 F 的最大可离域.

4) 假定 G_1 是 G 的子群，那么 $K_1=K(G)$ 中任意元的 p 次根如果在 K 中

必在 K_1 中.

5) $G(K(G_1))=G_1$.

6) 假定 K_1 中任意元的 p 次根在 K_1 中，那么 $K(G(K_1))=K_1$. 这就是说，定理 1 能够这样推广到不可离域.

§7.3 正 规 底

有穷次可离正规域的伽罗瓦理论包含四个主要定理，上节的定理 1 及定理 4 是其中两个，这节我们介绍其他两个. 因为正规底存在的证明较麻烦，所以这节大部分篇幅是介绍这证明.

假定 G 是由域 K 的 n 个自同构组成的群，F 是 K 中所有对于 G 中任意元不变动的元集合，显然 F 是 K 的子域. 这 G 是否就是 K 关于 F 的伽罗瓦群？假如我们能够证明 $(K:F)\leqslant n$，那么由 §5.6 定理 7，$(K:F)=n$，因此由 §5.6 定理 8，K 是 F 的可离域. 又因为 G 中元都是 K 的自同构. 于是根据 §5.5 定理 6，K 是 F 的 n 次可离正规域，所以 G 是 K 关于 F 的伽罗瓦群. 下面是伽罗瓦理论中第三个主要定理.

定理 1 假定 $G=\{\sigma_1,\cdots,\sigma_n\}$ 是由域 K 的自同构组成的群，F 是 K 中所有对于任意 σ_i 不变动的元形成的子域，那么 $(K:F)=n$；因此 G 是 K 关于 F 的伽罗瓦群.

这定理叫做**德狄享得**(I. W. R. Dedekind, 1831～1916)**定理**，有时又叫做**阿丁**(E. Artin, 1898～1962)**定理**.

证明 我们用反证法，假定 K 中 $n+1$ 个元 $\alpha_1,\cdots,\alpha_{n+1}$ 关于 F 线性无关，因为由 §4.1 定理 1，线性方程组

$$\sigma_i(\alpha_1)x_1+\sigma_i(\alpha_2)x_2+\cdots+\sigma_i(\alpha_{n+1})x_{n+1}=0, i=1,\cdots,n$$

在 K 中有非零解，那么这解不能在 F 中，否则 $\alpha_1,\cdots,\alpha_{n+1}$ 就线性相关，与假设不合. 假定

$$x_1=a_1,\cdots,x_{n+1}=a_{n+1}$$

是其中这样的一个解，它包含零的个数是最多的. 为了方便，我们

不妨假定 $a_i\neq 0, i<r, a_r=1, a_j=0, j>r$. 于是我们有

$$a_1\sigma_i(\alpha_1)+\cdots+a_{r-1}\sigma_i(\alpha_{r-1})+\sigma_i(\alpha_r)=0, i=1,\cdots,n.$$

再因为 $a_1,\cdots,a_{r-1}$ 不能都在 F 中，假定 $a_1\overline{\in}F$，并且 $\sigma_k(a_1)\neq a_1$，因此

$$\sigma_k(a_1)\sigma_k\sigma_i(\alpha_1)+\cdots+\sigma_k(a_{r-1})\sigma_k\sigma_i(\alpha_{r-1})+\sigma_k\sigma_i(\alpha_r)=0,$$

命 $\sigma_k\sigma_i=\sigma_j$，显然当 $i=1,\cdots,n$ 时，$j=1,\cdots,n$，于是

$$\sigma_k(a_1)\sigma_j(\alpha_1)+\cdots+\sigma_k(a_{r-1})\sigma_j(\alpha_{r-1})+\sigma_j(\alpha_r)=0$$

两式相减，得

$$\{a_1-\sigma_k(a_1)\}\sigma_i(\alpha_1)+\cdots+\{a_{r-1}-\sigma_k(a_{r-1})\}\sigma_i(\alpha_{r-1})=0$$

因为 $a_1-\sigma_k(a_1)\neq 0$，所以与上面 $a_1,\cdots,a_r$ 的挑选矛盾，因此定理成立.

定理 2 假定 G 是由域 K 的自同构组成的群，F 是 K 中所有对 G 中任意元不变动的元组成的子域，如果 $|G|=n$，那么 K 是 F 的 n 次可离正规域. 反过来，假如 K 是 F 的 n 次可离正规域，那么 $|G|=n$.

证明 假如 $|G|=n$，由定理 1 即得 K 是 F 的 n 次可离正规域. 假如 K 是 F 的 n 次可离正规域，那么 $|G|=n$，这是因为如果 $|G|<n$，由定理 1，$(K:F)<n$，这与假设不合，所以定理成立.

下面是正规底存在定理是伽罗瓦理论中第四个主要定理.

定理 3 假定 K 是 F 的 n 次可离正规域，$G=\{\sigma_1,\cdots,\sigma_n\}$ 是它的伽罗瓦群，那么 K 中有元 α，使

$$\sigma_1(\alpha),\sigma_2(\alpha),\cdots,\sigma_n(\alpha)$$

成为 K 关于 F 的底，这底我们叫做 K 关于 F 的正规底.

证明 我们知道，齐次线方程组有非零解的必要充分条件是：它的系数行列式不等于零，因此我们容易得知，K 中元 $\alpha_1,\cdots,\alpha_n$ 如果适合

$$\begin{vmatrix}\sigma_1^{-1}(\alpha_1)\cdots\sigma_1^{-1}(\alpha_n)\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \sigma_n^{-1}(\alpha_1)\cdots\sigma_n^{-1}(\alpha_n)\end{vmatrix}=|\sigma_i^{-1}(\alpha_j)|\neq 0,$$

那么,它们就关于 F 线性无关,因此也就是 K 关于 F 的底.于是 K 中元 α 如果适合 $|\sigma_i^{-1}(\sigma_j(\alpha))|\neq 0$,那么 $\sigma_1(\alpha),\cdots,\sigma_n(\alpha)$ 就是 F 的正规底.

现在分两段来证明 K 中的确存在着这样的元 α.

1. 当 F 是无穷域时.

假定 σ_1 是 G 的单位元,并且规定当 $\sigma_i^{-1}\sigma_j=\sigma_k$ 时,$(i,j)=k$,显然 $(i,1),\cdots,(i,n)$ 及 $(1,i),\cdots,(n,i)$ 都是 $1,\cdots,n$ 的排列,于是

$$f(x_1,\cdots,x_n)=\begin{vmatrix} x_{(1,1)}\cdots x_{(1,n)} \\ \cdots\cdots\cdots\cdots \\ x_{(n,1)}\cdots x_{(n,n)} \end{vmatrix}$$

是 $F[x_1,\cdots,x_n]$ 中的多项式.取 $x_1=1,x_i=0,i\neq 1$,因为 $(i,i)=1$,$(i,j)\neq 1,i\neq j$,显然

$$f(1,0,\cdots,0)=\begin{vmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{vmatrix}=1\neq 0,$$

因此 $f(x_1,\cdots,x_n)\neq 0$,即 $f(x_1,\cdots,x_n)$ 不恒等于零,但

$$f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))=\begin{vmatrix} \sigma_1^{-1}\sigma_1(\alpha)\cdots\sigma_1^{-1}\sigma_n(\alpha) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \sigma_n^{-1}\sigma_1(\alpha)\cdots\sigma_n^{-1}\sigma_n(\alpha) \end{vmatrix}$$

$$=|\sigma_i^{-1}\sigma_j(\alpha)|.$$

假如在 K 中我们能够找到元 α 使 $f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))\neq 0$,那么 $|\sigma_i^{-1}\sigma_j(\alpha)|\neq 0$,因此 $\sigma_1(\alpha),\cdots,\sigma_n(\alpha)$ 就是 K 关于 F 的正规底.

下面,我们在 K 中来找满足 $f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))\neq 0$ 的元 α.

假定 $\alpha_1,\cdots,\alpha_n$ 是 K 关于 F 的底,那么 $|\sigma_i(\alpha_j)|\neq 0$,于是命

(1) $$x_i=\sigma_i(\alpha_1)y_1+\cdots+\sigma_i(\alpha_n)y_n,\ i=1,\cdots,n,$$

我们有

$$f(x_1,\cdots,x_n)=f\left(\sum_{i=1}^n\sigma_1(\alpha_i)y_i,\cdots,\sum_{i=1}^n\sigma_n(\alpha_i)y_i\right)$$
$$=g(y_1,\cdots,y_n),$$

令(1)中 $x_1=1, x_i=0, i\neq 1$，由于 $|\sigma_i(\alpha_j)|\neq 0$，所以这时线性方程组(1)在 K 中有唯一组解 $\beta_1,\cdots,\beta_n$，因此

$$g(\beta_1,\cdots,\beta_n)=f(1,0,\cdots,0)\neq 0.$$

这就是说，$g(y_1,\cdots,y_n)\neq 0$. 再因为 $g(y_1,\cdots,y_n)$的系数是 K 中元，因为 K 是无穷域，由§3.10 习题 3，F 中有元 $a_1,\cdots,a_n$ 使得 $g(a_1,\cdots,a_n)\neq 0$，命

$$\alpha=\alpha_1 a_1+\cdots+\alpha_n a_n,$$

那么

$$f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))=f\Big(\sum_{i=1}^n\sigma_1(\alpha_i)a_i,\cdots,\sum_{i=1}^n\sigma_n(\alpha_i)a_i\Big)$$
$$=g(a_1,\cdots,a_n)\neq 0,$$

因此这时定理成立.

2. 当 F 是有穷域时.

由§7-1 定理 3，知 K 是 F 的循环域，如 $\alpha_1,\cdots,\alpha_n$ 是 K 关于 F 的底，σ 是 K 关于 F 的伽罗瓦群 G 的生成元，即 $G=(\sigma)$，命

$$\alpha=\sum_{i=1}^n a_i\alpha_i, a_i\in F,$$

那么

$$|\sigma^{-i}(\sigma^j(\alpha))|=|\sigma^{-i+j}(\alpha)|=\Big|\sum_{k=1}^n a_k\sigma^{-i+j}(\alpha_k)\Big|=|\beta_{-i+j}|,$$

这里
$$\beta_i=\sum_{j=1}^n a_j\sigma^i(\alpha_j), \beta_{i\pm n}=\beta_i.$$

假如在 K 中我们能够找出 α，也就是说，在 F 中能够找出 a_i 使多项式

$$g(x)=\sum_{i=0}^{n-1}\beta_i x^i$$

与 $f(x)=x^n-1$ 互质，那么 $\sigma_1(\alpha),\cdots,\sigma_n(\alpha)$就是正规底，这是因为这时在 $K[x]$中有满足

$$s(x)g(x)+t(x)(x^n-1)=1$$

的多项式 $s(x),t(x)$. 再我们取 n 阶矩阵

$$A\equiv A^1=\begin{bmatrix} 0 & 1 & & \text{\huge 0} \\ & \ddots & \ddots & \\ & \text{\huge 0} & \ddots & \ddots \\ 0 & & & 1 \\ 1 & 0 & & 0 \end{bmatrix}$$

其中大零表示它所在处未标出的矩阵元都是 0. 由计算我们容易得知

$$A^m=\begin{bmatrix} & & \overset{(m+1)}{1} & & \text{\huge 0} \\ & & & \ddots & \\ 1 & & \text{\huge 0} & & 1 \\ & \ddots & & & \\ \text{\huge 0} & & \underset{(m)}{1} & & \end{bmatrix},1<m<n,A^n=I.$$

把这 A 代上式的 x，即得矩阵等式 $s(A)g(A)=I$，于是

$$|s(A)||g(A)|=1,$$

但　$g(A)=\beta_0A^0+\beta_1A^1+\cdots+\beta_{n-1}A^{n-1}$

$$=\begin{bmatrix} \beta_0 & & \text{\huge 0} \\ & \ddots & \\ \text{\huge 0} & & \beta_0 \end{bmatrix}+\begin{bmatrix} 0 & \beta_1 & & \text{\huge 0} \\ & \ddots & \ddots & \\ & \text{\huge 0} & \ddots & \ddots \\ 0 & & & \beta_1 \\ \beta_1 & 0 & & 0 \end{bmatrix}+\cdots+$$

$$+\begin{bmatrix} 0 & & 0 & \beta_{n-1} \\ \beta_{n-1} & \ddots & & 0 \\ & \ddots & \text{\huge 0} & \\ \text{\huge 0} & & \beta_{n-1} & 0 \end{bmatrix}.=(\beta_{-i+j})$$

因此 $|\beta_{-i+j}|\neq 0$，所以 $\sigma_1(\alpha),\cdots,\sigma_n(\alpha)$ 是 K 关于 F 的正规底.

下面，我们来求使 $g(x)$ 与 $f(x)=x^n-1$ 互质的 a.

假定 $L(\supseteq K)$ 是 $f(x)=x^n-1$ 的分裂域，$b_1,\cdots,b_m(m\leqslant n)$ 是 $f(x)$ 在 L 中互异零点. 因为 $(L:F)\geqslant n$，在 L 中我们可以适当挑选 $b_{m+1},\cdots,b_n$，使 $b_1,\cdots,b_m,b_{m+1},\cdots,b_n$ 互异. 如果

$$g(b_i)\neq 0 \quad (i=1,2,\cdots,n),$$

那么 $g(x)$ 与 $f(x)$ 在 K 的扩张体中没有公共零点，因此 $g(x)$ 就是与 $f(x)$ 互质的了.

我们把 $g(b_j)$ 写成

$$g(b_j)=\sum_{i=1}^{n}a_i\Big(\sum_{k=0}^{n-1}\sigma^k(\alpha_i)b_j^k\Big)=\sum_{i=1}^{n}a_iq_{ij},\quad q_{ij}=\sum_{k=0}^{n-1}\sigma^k(\alpha_i)b_j^k.$$

因为 $\alpha_1,\cdots,\alpha_n$ 是 K 关于 F 的底，所以 $|\sigma^k(\alpha_i)|\neq 0$，又因为 $b_1,\cdots,b_n$ 互异，所以范得蒙行列式

$$|b_i^k|=\prod_{n\geqslant s>t\geqslant 1}(b_s-b_t)\neq 0.$$

因此，$|q_{ij}|=|\sigma^k(\alpha_i)||b_j^k|\neq 0$. 假定 $\gamma_1,\cdots,\gamma_r$ 是 L 关于 F 的底，

$$q_{ij}=\sum_{k=1}^{n}c_{ij}^{(k)}\gamma_k,c_{ij}^{(k)}\in F,i,j=1,\cdots,n.$$

因为 $|q_{ij}|=\sum_{\lambda_1,\cdots,\lambda_n=1}^{n}\gamma_{\lambda_1}\cdots\gamma_{\lambda_n}||c_{ij}^{(\lambda_k)}|$，所以其中有某个 $|c_{ij}^{(\lambda_k)}|\neq 0$. 于是在 F 中有满足

$$\sum_{i=1}^{n}a_ic_{ij}^{(\lambda_k)}=1,j=1,2,\cdots,n,$$

的元 a_i，如果这时

$$g(b_j)=\sum_{i=1}^{n}a_iq_{ij}=\sum_{k=1}^{r}\Big(\sum_{i=1}^{n}a_ic_{ij}^{(\lambda_k)}\Big)\gamma_k=0,$$

因为 $\gamma_1,\cdots,\gamma_r$ 关于 F 线性无关，那么 $\sum_{i=1}^{n}a_ic_{ij}^{(\lambda_k)}=0$，这与上面矛盾，所以 $g(b_j)\neq 0$. 这就是说，象上面这样挑选的 b_i 可以使 $g(x)$ 与 $f(x)$ 互质，因此定理得证.

这定理在 1932 年由多伊林(M. Deuring,1907～)首先证明，自后也还有其他证明，但直到 1950 年以前，所有这些证明都要引用表现理论. 虽然 1942 年阿丁有一个不引用表现理论的证明，但它只限于 F 不是有穷体的情形，因此不是一个完备的证明. 这里我们介绍的证明是 1950 年伽塞斯(J. W. S. Gasseis)及华尔(G. E.

Wall)提出的，它是一个不需要表现理论的初等证明[5].

§7.4　多项式能够用根号解出的条件

在复数域中，1，2，3，4 次多项式的零点都可以由复数用有理运算及根号来表出，这是我们早已知道的. 5 次及 5 次以上多项式的零点是否也能如此？这节就一般情形来讨论. 下面我们先讨论它的必要充分条件.

因为 x^n-a 的零点 α 我们常常叫做 a 的 n 次根，写成 $\sqrt[n]{a}$，因此 $F(\alpha)$ 又叫做 F 的根号扩张域. 又因为 $n=n_1n_2$ 时，$x^n-a=(x^{n_1})^{n_2}-a$ 的零点 可以看成 $x^{n_1}-\sqrt[n_2]{a}$ 的零点. 所以

$$\sqrt[n]{a}=\sqrt[n_1]{\sqrt[n_2]{a}}.$$

这样一来，我们就先引进下面的定义：

假设 K 是域 F 的扩张域，如果它们之间有中间体

$$F=F_0\subset F_1\subset\cdots\subset F_k=K, F_i=F_{i-1}(\alpha_i),$$

这里 $\alpha_i^{p_i}\in F_{i-1}$，$p_i$ 是质数，那么 K 就叫做 F 的**根号扩张域**. $F[x]$ 中多项式，如果它的分裂域是 F 的根号扩张域的子域，就叫做**能够用根号解出**.

为了方便，下面我们假定所需要的质数 p_i 次本原单位根都已包含在基础域 F 中，因此 F 的特征数异于 p_i.

要注意的是，F 的有穷次根号扩张域 $K=F_m$ 不一定是 F 的正规域，但可以再用根号来扩张使它成为 F 的正规域. 这是因为，首先，由于 p_1 次本原单位根在 F 中，所以 $f_1(x)=x^{p_1}-a_1, a_1\in F_1$ 的所有零点都在 $F_1=F(\alpha_1)$（α_1 是 $f_1(x)$ 的零点）中，也就是说，F_1 是 $f_1(x)$ 的分裂域，因此 F_1 是 F 的正规域. 如果 $K=F_1$，就是说 $m=1$，那么 K 就是 F 的正规域. 如果 $K\supset F_1$，就是说 $m\neq 1$，因为

$$F_2=F_1(\alpha_2),\quad \alpha_2 \text{ 是 } x^{p_2}-a_2, a_2\in F_1 \text{ 的零点},$$

这时 F_2 不一定是 F 的正规域. 下面我们来作包含 F_2 的 F 的正规

域. 命 σ 是 F_1 关于 F 的伽罗瓦群中的任意元，那么

$$f_2(x)=\prod_{\sigma}(x^{p_2}-\sigma(a_2))$$

是 $F[x]$中多项式. 我们把 $f_1(x)f_2(x)$的零点添加于 F 就得到 F_2 的扩张域的 L_2，因为 F 包含 p_2 次本原单位根，所以 L_2 是 $F[x]$中多项式 $f_1(x)f_2(x)$的分裂域，因此是 F 的正规域. 如果 $K\subseteq L_2$，就是说，$m=2$，那么 L_2 就是所求的正规域；如果 K 不是 L_2 的子域，即 $m>2$，因为 $F_3=F_2(a_3)$，$x^{p_3}-a_3\in F_2[x]\subseteq L_2(x)$，设 σ_2 是 L_2 关于 F 的伽罗瓦群中任意元，那么

$$f_3(x)=\prod_{\sigma_2}(x^{p_3}-\sigma_2(a_3))\in F[x].$$

把 $f_1(x)f_2(x)f_3(x)$的零点添加于 F 得到 L_3，显然 $L_3\supseteq F_3$，并且 L_3 是 F 的正规域，如果 $m=3$，那么 L_3 就是所求的域，如果 $m>3$，我们用同样方法继续添加根号，经过有穷回后，终可得到包含 K 的 F 的正规域 L. 这就是说，假如 K 是 F 的根号扩张域，那么存在 F 的根号扩张域 $L\supseteq K$，并且 L 是 F 的正规域.

我们先证明 § 7.1 定理 2 的逆定理以备引用.

定理 1 假定域 F 含有 n 次本原单位根 ξ，K 是 F 的 n 次循环域，那么 $K=F(\gamma)$，这里 γ 是纯多项式 $x^n-a\in F[x]$的零点.

证明 假定 σ 是 K 关于 F 的伽罗瓦群 G 的生成元，即 $G=(\sigma)$. 根据 § 7.3 正规底定理，我们有元 $\alpha\in K$，使

$$\beta=\alpha+\xi\sigma(\alpha)+\cdots+\xi^{n-1}\sigma^{n-1}(\alpha)\neq 0.$$

因为 $\sigma^n(\alpha)=\alpha$，所以

$$\begin{aligned}\sigma(\beta)&=\sigma(\alpha)+\xi\sigma^2(\alpha)+\cdots+\xi^{n-1}\sigma^n(\alpha)\\&=\xi^{-1}\{\xi\sigma(\alpha)+\xi^2\sigma^2(\alpha)+\cdots+\alpha\}=\xi^{-1}\beta\end{aligned}$$

一般 $\sigma^i(\beta)=\xi^{-i}\beta$，$i=1,\cdots,n-1$. 因此

$$\sigma^i(\beta)\neq\sigma^j(\beta),\ i\neq j.$$

于是 β 有 n 个互异的共轭元，所以它们是同一既约多项式的零点，这既约多项式显然是 n 次的. 因此 $K=F(\beta)$. 再因为

$$\sigma(\beta^n)=(\sigma(\beta))^n=\beta^n,$$

所以 $\beta^n\in F$，命 $\beta^n=a$，那么 β 是纯既约多项式 x^n-a 的零点，因此定理成立.

要注意的是，定理中 n 不能用 F 的特征数 p 整除，因为如果不如此，首先 F 的 n 次本原单位根不存在. 再 x^n-a 的零点是重零点，把它添加于 F 得到的域不是可离域.

下面是多项式能够用根号解出的必要条件，这里的多项式我们假定是可离的.

定理 2　假定 $F[x]$ 中多项式 $f(x)$ 能够用根号解出，并且 F 的特征数不能整除根号的次数，那么它的伽罗瓦群是可解群.

证明　假设 K 是 $f(x)$ 的分裂体，因为 $f(x)$ 能够用根号解出，所以 K 是 F 的根号扩张域的子域. 由前面的讨论，我们得知 K 有这样的扩张域 L 存在，它是 F 的正规域，并且在它与 F 之间有中间体

$$F=F_0\subset F_1\subset\cdots\subset F_k=L,$$

这里 $F_i=F_{i-1}(\alpha_i)$，$\alpha_i^{p_i}\in F_{i-1}$，因为 F 含有 p_i 次本原单位根，所以 F_i 是 F_{i-1} 的正规域. 假设 G 是 L 关于 F 的伽罗瓦群，G_i 是 F_i 所属的子群，于是我们有

$$G=G_0\supset G_1\supset\cdots\supset G_k=E.$$

因为 F_i 是 F_{i-1} 的正规域，所以 $G_i\lhd G_{i-1}$，且 G_{i-1}/G_i 是 F_i 关于 F_{i-1} 的伽罗瓦群，因此 G_{i-1}/G_i 的元数是 p_i. 于是它是循环群，也就是交换群，所以 G 是可解群. 但 K 是 F 的正规域，因此 $G/G(K)$ 是 K 关于 F 的伽罗瓦群，也就是 $f(x)$ 的伽罗瓦群. 因为 G 是可解群，由 §6.3 定理 9，商群 $G/G(K)$ 也是可解群，所以 $f(x)$ 的伽罗瓦群是可解群，因此定理成立.

在上面的定理中，如果 F 的特征数能够整除根号的次数，那么 $f(x)$ 的分裂域 K 是 F 的不可离域，这时它的伽罗瓦群就不在我们讨论范围内.

现在，我们来证明根号解出的充分条件.

定理 3　假定 $F[x]$ 中多项式 $f(x)$ 的伽罗瓦群 G 是可解群，

并且 F 的特征数不能整除 G 的元数，那么 $f(x)$ 能够用根号解出.

证明 我们知道，假如群 $A\supset B\supset C$，其中 B,C 都是 A 的正规子群，如果 A/C 是交换群，由 § 6.2 第一同构定理，

$$A/B\simeq(A/C)/(B/C)$$

所以 A/B 是交换群. 再因为交换群只有元数是 1 或是质数时才是单群. 于是我们容易得知，这时 K 关于 F 的伽罗瓦群 G 有这样的合成群列

$$G=G_0\supset G_1\supset\cdots\supset G_k=E,$$

其中商群 G_{i-1}/G_i 是元数为质数 p_i 的循环群. 命 F_i 是 K 中属于 G_i 的子域，于是我们有

$$F=F_0\subset F_1\subset\cdots\subset F_k=K.$$

因为 G_{i-1} 是 G_i 的正规子群，所以 F_i 是 F_{i-1} 的正规域. 再因为 F_i 关于 F_{i-1} 的伽罗瓦群 G_{i-1}/G_i 是 p_i 次循环群，所以 F_i 是 F_{i-1} 的 p_i 次循环域. 但我们已假定 F 中含有 p_i 次本原单位根(因此 F 的特征数异于 p_i)，由定理 1，$F_i=F_{i-1}(\alpha_i)$，这里 $\alpha_i^{p_i}\in F_{i-1}$，所以 K 是 F 的根号扩张域，因此 $f(x)$ 能够用根号解出，所以定理得证.

我们要注意的是，在上面定理中，如果没有 F 的特征数不能整除 $|G|$ 的这条件，那么定理 1 不能引用，因此定理就不能成立. 也就是说，多项式 $f(x)$ 的伽罗瓦群虽是可解群，如果 F 的特征数与 $|G|$ 不互质，那么 $f(x)$ 不一定能够用根号解出. 譬如，假定 F 是特征数为 2 的质域，$\{u,v\}$ 关于 F 代数无关，$K=F(u,v)$ 是 F 的超越域，那么 2 次多项式

$$f(x)=x^2+ux+v$$

显然是可离的，因此 $f(x)$ 的分裂域是 K 的 2 次可离域，于是 $f(x)$ 的伽罗瓦群的元数是 2，所以它是可解群. 但是添加奇数次纯多项式的零点于 K 得到的扩张域关于 K 是奇数次，添加偶数次纯多项式的零点于 K 得到的扩张域是 K 的不可离域，因此 $f(x)$ 的分裂域不可能是 K 的根号扩张域的子域，这就是说，$f(x)$ 不能够用根号解出.

在上面讨论中，我们假定 F 含所需要的质数 p_i 次本原单位根只是为了方便，如果没有这假定，上面的定理 2 及定理 3 仍然是同样成立的，其理由如下：

假如 $f(x)$ 的分裂域 K 是 F 的根号扩张域 L 的子域，因为 F 的特征数不能整除根号的次数，所以 F 有 $(L:F)$ 次本原单位根，我们把它添加于 K 得到域 K'，添加于 F 得到域 F'，于是 $K'\supseteq F'\supseteq F$，这时 K' 是 F 的正规域，因此 K' 也是 F' 的正规域. 命 K' 关于 F 及 F' 的伽罗瓦群分别是 G 及 G'，因为 F' 是 F 的正规域，所以 G' 是 G 的正规子群，显然 K' 是 F' 的根号扩张域的子域，由定理 2，G' 是可解群. 再因为 G/G' 是 F' 关于 F 的伽罗瓦群，由 §7.1，它是交换群，因此 G 是可解群(§6.3 习题 2)，但 $f(x)$ 的伽罗瓦群是 $G/G(K)$，它是可解群 G 的商群，所以 $f(x)$ 的伽罗瓦群是可解群.

再假如 $f(x)$ 的分裂域是

$$K=F(\alpha_1,\cdots,\alpha_n),$$

它的伽罗瓦群 G 是可解群，元数是 m. 因为 F 的特征数不能整除 m，所以 F 的 m 次本原单位根存在. 假定把它添加于 F 得到的域是 F'，那么

$$K'=F'(\alpha_1,\cdots,\alpha_n)$$

是把 $f(x)$ 看成 $F'[x]$ 中多项式时的分裂域，假如能证明 K' 关于 F' 的伽罗瓦群 G' 是 G 的子群，那么 G' 是可解群，因为 $|G'|$ 是 $|G|$ 的因数，所以 F' 的特征数不能整除 $|G'|$. 于是由定理 3，K' 是 F' 的根号扩张域的子域，因此也是 F 的根号扩张域的子域，所以 K 是 F 的根号扩张域的子域. 我们知道，G' 中任意元把 α_i 变为 α_j，也就是说，它决定 $\alpha_1,\cdots,\alpha_n$ 的一个排列，并且它不使 F' 中元变动，因此也不使 F 中任意元变动，所以它又决定 G 中一元. 再因为 G' 中两个不同的元所决定 $\alpha_1,\cdots,\alpha_n$ 的排列不同，因此，它所决定的 G 中元也不同. 于是，G' 与 G 的子群同构，所以 G' 可以看成 G 的子群.

§7.5 多项式的解

我们先讨论一般多项式的解.

假定$F(u_1,\cdots,u_n)$是域F的超越扩张域,u_i是

$$F(u_1,\cdots,u_{i-1},u_{i+1},\cdots,u_n)$$

的超越元,也就是说,超越元集$\{u_1,\cdots,u_n\}$关于F代数无关,那么n次多项式

$$f(x)=x^n-u_1x^{n-1}+u_2x^{n-2}-\cdots+(-1)^nu_n$$

就叫做F的n次一般多项式,或简称n次**一般多项式**.

假如$v_1,\cdots,v_n$是$f(x)$在它的分裂域K中的零点,那么

$$u_1=v_1+\cdots+v_n,u_2=v_1v_2+\cdots+v_{n-1}v_n,\cdots,$$

$$u_n=v_1v_2\cdots v_n,$$

显然$F(v_1,\cdots,v_n)$是$F(u_1,\cdots,u_n)$的扩张域,因此

$$K=F(v_1,\cdots,v_n).$$

再$\{v_1,\cdots,v_n\}$关于F也代数无关,这因为如果$\{v_1,\cdots,v_n\}$关于F代数相关,设v_1关于F与$\{v_2,\cdots,v_n\}$代数相关,置

$$L=F(v_2,\cdots,v_n),$$

那么$L(v_1)$是L的代数域,因为$u_i\in L(v_i)$,所以u_i都是L的代数元,即u_i关于F与$v_2,\cdots,v_n$代数相关,但$u_1,\cdots,u_n$关于F代数无关,这与§5.9中性质5矛盾.下面论述著名的**阿贝耳定理**.

定理1. n次一般多项式$f(x)$的伽罗瓦群是它的n个互异零点上或n个文字上的对称群S_n.

证明 $f(x)$的伽罗瓦群G中元是不使$F(u_1,\cdots,u_n)$中任意元变动的$F(v_1,\cdots,v_n)$的自同构,它不使$f(x)$的任意系数u_i变动,因此它把$f(x)$的零点仍然变为$f(x)$的零点,所以它决定$v_1,\cdots,v_n$的一个排列.G中不同的元决定不同的排列.反过来,$v_1,\cdots,v_n$的任意一个排列,因为$v_1,\cdots,v_n$都是超越元,也就是说,它们都是记号或者都是文字,我们容易得知,它产生$F(v_1,\cdots,v_n)$的一个自

同构，这自同构不使 $u_1,\cdots,u_n$ 变动，因此也不使 $F(u_1,\cdots,u_n)$ 中任意元变动，所以 $v_1,\cdots,v_n$ 的任意一个排列决定 G 中一元，于是 G 是 n 个文字 $v_1,\cdots,v_n$ 上的对称群 S_n. 因此定理得证.

我们知道对称群 S_n 当 $n\leqslant 4$ 时是可解群，当 $n\geqslant 5$ 时不是可解群. 所以当 F 的特征数不是 2 或 3 时，$F[x]$中 5 次以下的多项式都能够用根号解出. 4 次以上的一般多项式不能用根号解出，即

定理 2 n 次一般多项式当 $n\geqslant 5$ 时，不能够用根号解出.

要注意的是，这里讨论的虽然是一般多项式，但是 4 次以上的多项式即使系数是整数的也不一定都能够用根号解出，后面习题 3 就是一个显明的例.

再我们知道，多项式的伽罗瓦群是它零点上的对称群，或者是对称群的子群.既约多项式的伽罗瓦群是它零点的可迁群. 下面，我们来讨论怎样的可迁群才是可解群？

我们先介绍一个定义以备引用.

假设 σ 是数字 $1,2,\cdots,n$ 的排列，如果有整数 $a(\not\equiv 0(\bmod n))$，b，使

$$\sigma(i)\equiv ai+b(\bmod n),i=1,2,\cdots,n,$$

那么 σ 叫做关于 n 的**线性变换**. 当 $a=1,b\neq 0$ 时，$\sigma(i)\equiv i+b$ 使任意数变动，因此它是 n 个文字上的循环排列.

下面是我们需要的定理.

定理 3 假定 $f(x)$ 是 $F[x]$中质数 p 次的既约多项式，它的伽罗瓦群 G 是$\{1,2,\cdots,p\}$的可迁群，那么 G 是可解群的必要充分条件是：把 $1,2,\cdots,p$ 的顺序适当改写；G 中任意元 τ 是关于 p 的线性变换，即 $\tau(i)\equiv ai+b(\bmod p)$，并且 G 包含线性变换

$$\sigma(i)\equiv i+1(\bmod p).$$

证明 我们先用归纳法证明必要性.

假如 G 是可解群，

$$G=G_0\supset G_1\supset\cdots\supset G_{k-1}\supset G_k=E$$

是它的正规群列，并且 G_{i-1}/G_i 是交换群，这时我们可以假定 G_{k-1}

是循环群，因为如果不是如此，任取它的一个循环子群插入 G_{k-1}、G_k 之间就能成为这样的正规群列. 再因为 G 是 $\{1,2,\cdots,p\}$ 的可迁群，G_1 是 G 的正规子群，由 §6.6 定理 2，G_1 也是 $\{1,2,\cdots,p\}$ 的可迁群，因此 $G_2,\cdots,G_{k-1}$ 都是 $\{1,2,\cdots,p\}$ 的可迁群.

下面，我们先证明 G_{k-1} 中元都是关于 p 的线性变换. 假定 σ 是 G_{k-1} 的生成元，即 $G_{k-1}=(\sigma)$，那么 σ 是 p 个数字的循环排列. 这是因为，如果 $\sigma=(1ij\cdots m)(n\cdots q)$，$\sigma$ 的乘幂只能把 1 变为 $1,i,j,\cdots,m$，而不能把 1 变为 $n,\cdots,q$，这与 $G_{k-1}=(\sigma)$ 是可迁群的性质不合，因此如果把 $1,2,\cdots,p$ 的顺序适当改写，我们就有

$$\sigma(i)\equiv i+1(p),$$

于是 $\sigma^r(i)\equiv i+r(p)$，$r=1,2,\cdots,p$. 即 G_{k-1} 中任意元都是关于 p 的线性变换.

再假设 τ 是 G_{k-2} 中任意元，因为 G_{k-1} 是 G_{k-2} 的正规子群，所以 $\tau\sigma\tau^{-1}\in G_{k-1}$，我们命 $\tau\sigma\tau^{-1}=\sigma^a$，$\tau(i)=j$，因此

$$\tau\sigma\tau^{-1}(j)=\sigma^a(j)\equiv j+a(p),$$

于是

$$\tau\sigma(i)=\sigma^a\tau(i)\equiv\tau(i)+a(p).$$

也就是说，对任意 i，我们有

$$\tau(i+1)\equiv\tau(i)+a(p).$$

假如令 $\tau(1)\equiv b+a(p)$，那么

$$\tau(i)\equiv b+ai(p),\ i=1,2,\cdots,p.$$

这就是说，G_{k-2} 中任意元是关于 p 的线性变换. 又因为当 $a\not\equiv1(p)$ 时，有适合 $b+ai\equiv i(p)$，即 $(a-1)i\equiv-b(p)$ 的数 i 存在，所以只有 $\tau(i)\equiv b+i(p)$ 使任意数字变动，但 $\tau=\sigma^b$，因此 G_{k-2} 中使任意数字变动的排列是 G_{k-1} 中排列，也就是说，G_{k-2} 中任意 p 项循环排列是 G_{k-1} 中排列.

现在，我们假设 G_{k-n} 有 G_{k-2} 的性质，即 G_{k-n} 中任意排列是关于 p 的线性变换，并且 G_{k-n} 中任意 p 项循环排列是 G_{k-1} 中排列，如果 τ 是 G_{k-n-1} 中任意排列，因为 σ 是 p 项循环排列，由 §2.2，$\tau\sigma\tau^{-1}$ 是 G_{k-n} 中 p 项循环排列，因此在 G_{k-1} 中. 于是 $\tau\sigma\tau^{-1}=\sigma^a$. 同

上面一样，我们有 $\tau(i)\equiv ai+b(p)$，因此 G_{k-n-1} 中任意元是关于 p 的线性变换，并且其中任意 p 项循环排列是 G_{k-1} 中排列，由归纳法我们得知必要条件成立.

下面，我们来证明充分性.

假定 G 是由关于 p 的线性变换组成的群，并且含有线性变换 $\sigma(i)=i+1(p)$，N 是 σ 生成的循环子群，如果能够证明 N 是正规子群，并且 G/N 是可解群，那么 G 就是可解群了. 因为 G 中使任意数字变动的排列是 σ^{h}，所以它们都是 N 中排列，也就是说，G 中任意 p 项循环排列都在 N 中. 但用 G 中任意排列把 N 中任意排列变形(§2.4)得到的排列仍然是 p 项循环排列，因此也是 N 中排列，所以 N 是 G 的正规子群. 假如 $\tau(i)\equiv ai+b(p)$ 是 G 中任意元，那么在陪集 τN 中有元

$$\tau\sigma^{r}(i)\equiv ai+ar+b\equiv ai(p),$$

这里 $ar+b\equiv 0(p)$，假如命 τ 与 a 对应，我们很容易证明这对应是 G/N 到 $\bar{Z}=Z-(p)$ 的乘群内的同构，所以 G/N 与 $\bar{Z}$ 的乘群的子群同构. 于是 G/N 是交换群. 因此 G 是可解群. 充分条件成立.

定理证毕.

一个关于质数 p 的线性变换 $\sigma(i)\equiv ai+b(p)$ 除不动排列外，最多只能够使一个数字不变动. 这是因为，同余式 $i\equiv ai+b(p)$，即

$$(a-1)i\equiv -b(p),$$

除 $a\equiv 1, b\equiv 0$ 即恒等变换外，只能有一个解. 因此，假如线性变换能使两个数字不变动，那么它就使任意数字不变动了.

下面是一个常常引用的重要定理.

定理 4 假如系数是实数的质数次既约多项式 $f(x)$ 能够用根号解出，那么它的零点只能有一个是实数或者全部都是实数.

证明 假如 $f(x)$ 的分裂域 K 含有复数，因为 K 是正规域，所以共轭复数也在 K 中，因此 K 中任意数与它的共轭元对应是不使 K 中实数变动的 K 的自同构，显然它是 $f(x)$ 的伽罗瓦群 G 中元. 这元不是 G 的单位元，由定理 3，它不能使两个零点不变动，所

以如果 $f(x)$ 的零点不都是实数，那么它只能有一个零点是实数，因此定理得证.

习 题 7.5

1. 假如已知 $n\geqslant 5$ 时交代群 A_n 是单群，试用这性质证明对称群 S_n 不是可解群.

2. 5 次实系数既约多项式如果只有三个实根，它就不能够用根号解出.

3. 试证多项式 x^5-4x+2 不能够用根号解出.

§7.6 用圆规与直尺的作图

假如我们已经知道平面上有穷个初等几何图形(点、直线、圆等)，要求用圆规及直尺来作出适合已给条件的初等几何图形，这要求在什么条件下才能实现？当然这条件是包含那些已知的初等几何图形. 这节我们就是解答这问题.

我们知道，在用圆规及直尺作图的过程中，在已知范围内可以任意挑选一点，过两点可以作一直线，已知圆心及半径可以作一圆. 假如两直线、两圆或一直线一圆能够作出，那么它们的交点也能够作出. 一个初等几何图形能够作出，只不过是重复引用上面的方法作出一些适当的点，直线，圆罢了.

因为直线同圆都可以用点来决定，所以用圆规与直尺的作图问题可以看成是由已知点作出适合某些条件的点的问题. 假如我们引用坐标，把点换成数，那么作点的问题就变为作数的问题了. 假如数 $a,b,c,\cdots$ 是决定已知图形的点的坐标，因为它们中任意两数的和、差、积、商都能作出，所以体 $F=Q(a,b,c,\cdots)$ 中数都能够作出，这里 Q 是有理数域.

现在我们来讨论初等几何图形能够用圆规与直尺作出的条件.

我们知道，一点如果能够任意挑选，我们可以假定它的坐标是

有理数. 过坐标是 F 中数的两点的直线，它的方程的系数也是 F 中数，因此这样的两条直线的交点的坐标又是 F 中数. 如果圆上的三个点，或一个点及它的圆心，它们的坐标都是 F 中数，那么这圆的方程的系数也是 F 中数. 但是方程的系数是 F 中数的两圆或一圆一直线，它们交点的坐标一般含有 F 中数的平方根，所以不一定是 F 中数. 于是假如数 x 能够作出，也就是说，x 是方程的系数为 F 中数的某些直线及圆的交点，那么 x 能够用 F 中数的有理运算及平方根号表示. 反过来显然也成立，这是因为我们根据 $1:b=b:a$ 可以作出已知数 a 的平方根 $b=\sqrt{a}$. 于是我们有

定理 1 数 x 能够用圆规与直尺作出的必要充分条件是它能够用 F 中数的有理运算及平方根号表示.

但是，怎样的数才能够用 F 中数的有理运算及平方根来表出？我们又如何来判别？

假如数 x 能够用 F 中数的有理运算及平方根表示，那么它就在陆续添加平方根于 F 形成的域中. 同 §7.4 中讨论的一样，这域可以再用平方根来扩张使它成为 F 的正规域 K，即

$$K=F_m\supset F_{m-1}\supset\cdots\supset F_0=F,$$

这里 F_i 是 F_{i-1} 中纯多项式 x^2-a_i 的分裂域，因为 $(F_i:F_{i-1})=2$，根据 §5.3 定理 4，我们有

$$(K:F)=(F_m:F_{m-1})\cdots(F_1:F)=2^m.$$

反过来，假如 x 在 F 的正规域 K 中，并且 $(K:F)=2^m$，那么 K 关于 F 的伽罗瓦群 G 的元数是 2^m，因此由 §6.3 定理 11，G 是可解群. 我们知道有穷群有合成群列，元数是 p^n 的群只有 $n=1$ 时才是单群，因此 G 有商群的元数都是 2 的合成群列

$$K=F_m\supset F_{m-1}\supset\cdots\supset F_0=F,$$

这时 $(F_i:F_{i-1})=2$，所以 x 能够用 F 中数的有理运算及平方根表出. 因此我们有

定理 2 数 x 能够用圆规与直尺作出的必要充分条件是它在关于 F 次数为 2^m 的正规域中.

下面，我们来讨论三个古典的初等几何作图问题，以作结束.

首先是圆的求积问题. 假如我们取圆的半径为1，那么求作与圆的面积相等的正方形就是求作 π，但 π 是超越数[6]，显然不能用有理数及有理数的平方根表示. 因此它不能用圆规与直尺作出.

其次是立方倍积问题. 假如我们取立方体的一边长作为1，那么要作的数 x 应适合条件 $x^3-2=0$，这多项式的零点不是有理数. 如果命 α 是它的零点，那么 $(Q(\alpha):Q)=3$，所以 α 不在有理数域 Q 的 2^m 次扩张域中，因此 x 不能够用圆规与直尺作出.

最后是任意角三等分问题. 假如 α 是任意角，θ 是所求角，因为 $\alpha=3\theta$，由三角公式，得

$$\cos\alpha=\cos 3\theta=4\cos^3\theta-3\cos\theta.$$

命 $\cos\alpha=\frac{a}{2}$，$\cos\theta=\frac{x}{2}$，那么 x 适合的条件是

$$4\left(\frac{x}{2}\right)^3-3\cdot\frac{x}{2}=\frac{a}{2},$$

即

$$x^3-3x-a=0.$$

如果取 $\alpha=60°$，那么 $a=1$. 但 $x^3-3x-1=0$ 没有是有理数的零点，假如把它的零点添加于有理数域 Q 得到的域是 K，那么

$$(K:Q)=3,$$

所以 x 不能用圆规与直尺作出. 因此 θ 也不能够用圆规与直尺作出.

参 考 文 献

[1] 熊全淹，初等整数论（再版），湖北教育出版社(1988).

[2] Granville McCormick, A theorem on finite abelian groups, Amer. Math. Monthly, 67(1960), 670.

[3] Find Galois group of equation $x^9-x^3+1=0$ over rationals, Amer. Math. Monthly, 85(1978), 597~598.

[4] T. Nakavama (中山正) Generalized Galois theory of rings with mini-

mum condition, I, Amer, Jour. of Math., 73(1951), 1～12; II, Amer. Jour. of Math., 77(1955), 1～16.

[5] M. Deuring, *Galoische Theorie und Darstellungstheoric*, Math. Ann., 107(1932), 140～144.

E. Artin, Galois Theory, (1946), 66～67.

J. W. S. Gasseis and G. E. Wall, The normal basis theorem, Jour. of London Math. Soc., 25(1950), 250～264.

[6] I. Niven, A simple proof that π is irrational, Bull. Amer. Math. Soc., 53(1947), 509.

第8章

环　　论

环构造的研究可以说是从1908年魏特邦关于有穷次代数构造的著名论文[1]开始的.经过一个较长时间,进展不大;到了30年代魏特邦定理才得到推广.1927年阿丁提出了用极小条件来区别环.阿丁把魏特邦定理推广到满足极小条件的环[2],基本上奠定了满足极小条件环构造的基础,因此满足极小条件的环叫做阿丁环.在40年代开始研究不满足极小条件的环.1945年贾柯勃逊创造根基理论,把魏特邦定理进一步推广到一般不满足极小条件的环[3],建立了一般环构造的基础理论.在50年代提出了各种不同的根基理论[4],互有短长.但应用时一般多以贾柯勃逊理论为主.

目前,介绍环构造的书籍为数不少,其中内容丰富涉及面又广的要以1956年贾柯勃逊所著《环构造》[5]为最,只是起点较高,叙述过简,初学难以领会.拙编《环构造》内容较全,论证亦详,可供参考.

这章主要讨论环的构造,分7节,前四节讨论满足极小条件环的构造,也就是阿丁环的构造.后三节根据贾柯勃逊根基,讨论一般环的构造。

§8.1　阿　丁　环

1927年阿丁把1908年魏特邦的有穷次代数构造定理推广到满足极小条件的环,这些定理叫做魏特邦–阿丁定理.这章前四节主要是介绍这些定理.为了叙述方便,今后两节先介绍基本概念及

性质，以备引用.

假定 R 是环，如果它的任意左理想列

$$L_1 \supset L_2 \supset \cdots \supset L_n \supset \cdots,$$

L_i 是 R 的左理想，只有有穷项，也就是说，对于任意含无穷项的左理想列

$$L_1 \supseteq L_2 \supseteq \cdots \supseteq L_n \supseteq \cdots,$$

必定存在一个正整数 m，自 m 项后的所有左理想都相等，即

$$L_m = L_{m+1} = \cdots,$$

那么 R 叫做满足(左理想)**降链条件**.

假如 R 是满足降链条件的环，那么，在它的任意左理想的集合中，有不包含这集合中其他左理想的左理想，也就是说，任意左理想集合中含有它的极小左理想(可能不只一个)，这是因为，假如 L_1 是这集合中左理想，如果它不是这集合的极小左理想. 那么，在这集中有包含于 L_1 的左理想 L_2，于是我们有 $L_1 \supset L_2$. 如果 L_2 又不是极小左理想，我们又有 $L_1 \supset L_2 \supset L_3$，这样继续下去，我们就得到左理想列

$$L_1 \supset L_2 \supset L_3 \supset \cdots \supset L_i \supset \cdots,$$

因为它只能有穷项，所以最后的 L_m 就不包含这集中其他左理想，因此 L_m 就是这集合的极小左理想. 一个环 R，如果它的任意左理想集都有极小左理想，我们就说 R 满足(左理想)**极小条件**. 因此，一个环如果满足降链条件，它也满足极小条件. 反过来，如果环满足极小条件，那么 $L_1 \supset L_2 \supset \cdots \supset L_n \supset \cdots$ 只能有穷项，否则就不满足极小条件，因此 R 也满足降链条件. 极小条件是降链条件的另一表达形式. 满足极小条件或者说满足降链条件的环，叫做**阿丁环**

譬如，有穷环显然满足极小条件，所以它是阿丁环. 再因为体只有两个左理想，所以体也是满足极小条件的环，因此体也是阿丁环. 假如 R 是阿丁环，那么 R^n 也是阿丁环，这里 n 是正整数[7]. 同样，假定 A 是代数，如果 A 满足左理想的降链条件，那么 A 叫做**阿丁代数**，譬如 A 是域 F 有穷次代数，因为 A 的左理想 L_i 是 A

的子空间，并且当 $L_i \supset L_j$ 时，L_i 的维数大于 L_j 的维数，所以 A 满足极小条件.因此 A 是阿丁代数，假如 A 只看成环，那么 A 不一定满足极小条件.于是一个代数如果是阿丁代数，它不一定是阿丁环.如果是阿丁环，显然它又是阿丁代数，再整数环不是阿丁环，因为

$$(m)\supset(2m)\supset(2^2m)\supset\cdots$$

就是含无穷项的理想列，即它不满足降链条件.同样，主理想环以及多项式环都不是阿丁环.又全矩阵环 Z_2 也不是阿丁环，因为下面的左理想列有无穷项

$$L_1\supset L_2\supset\cdots\supset L_n\supset\cdots$$

这里 L_i 是所有形如

$$\begin{pmatrix} 2^i a & 0 \\ 2^i b & 0 \end{pmatrix}, a, b \text{ 是整数}$$

的矩阵组成的左理想.所以阿丁环是一个比较特殊的环，即极小条件是一个很强的条件，就是最普通的整数环也不满足这条件.

由定义得知阿丁环 R 的左理想包含 R 的极小左理想.阿丁环的子环不一定是阿丁环，但阿丁代数的子代数仍然是阿丁代数.

同样，对于模也有降链条件或极小条件.设 M 是环 R-模，如果 M 的任意降链子模列只有有穷项，或 M 的任意子模集有极小子模，那么 M 叫做阿丁模.显然假如 R 是阿丁环，那么 ${}_RR$ 是阿丁模.阿丁模的子模是阿丁模.

下面我们介绍阿丁环的几个基本性质.

定理 1 假定环 R 是阿丁环，那么同余环 $\bar{R}=R-N$ 也是阿丁环，这就是说，阿丁环的同态象也是阿丁环.

证明 假定 $\bar{L}_1\supseteq\bar{L}_2\supseteq\cdots\supseteq\bar{L}_n\supseteq\cdots$

是同余环 $\bar{R}$ 的任意左理想列，因为 $R\sim\bar{R}$，所以 $\bar{L}_i$ 在 R 的完全象源 L_i 是 R 的左理想，因此

$$L_1\supseteq L_2\supseteq\cdots\supseteq L_n\supseteq\cdots$$

是 R 的左理想列，但 R 满足极小条件，所以 $L_m=L_{m+1}=\cdots$于是

$$\bar{L}_m=\bar{L}_{m+1}=\cdots,$$

这就是说，$\bar{R}$ 满足极小条件，所以定理成立.

上定理的逆不一定成立，即 $\bar{R}=R-N$ 是阿丁环时，R 不一定是阿丁环. 譬如，整数环 Z 不是阿丁环，而 $\bar{Z}_m=Z-(m)$ 只有 m 个元，是有穷环，当然是阿丁环. 但我们有下定理.

定理 2 假定 N 是环 R 的理想，如果 N 及 $\bar{R}=R-N$ 都是阿丁环，那么 R 也是阿丁环.

证明 假定 $L_1\supseteq L_2\supseteq\cdots\supseteq L_n\supseteq\cdots$ 是 R 的任意左理想列，那么

$$(L_1\cap N)\supseteq(L_2\cap N)\supseteq\cdots\supseteq(L_n\cap N)\supseteq\cdots,$$

是 N 的左理想列，再因为 $R\sim\bar{R}=R-N$，而 L_i 在 $\bar{R}$ 的象 $\bar{L}_i$ 是 $\bar{R}$ 的左理想，因此

$$\bar{L}_1\supseteq\bar{L}_2\supseteq\cdots\supseteq\bar{L}_n\supseteq\cdots$$

是 $\bar{R}$ 的左理想列. 由假设这两个左理想列都只能有穷项，因此存在着正整数 m，使得

$$L_t\cap N=L_m\cap N,\bar{L}_t=\bar{L}_m,t\geqslant m$$

下面我们来证明 $L_t=L_m$. 因为 $L_t\subseteq L_m$，根据 §1.1 定理我们有

$$\begin{aligned}L_t&=L_t\cap(L_t\cup N)=L_t\cap(L_m\cup N)\\&=L_m\cup(I_t\cap N)=L_m\cup(L_m\cap N)=L_m.\end{aligned}$$

定理证毕.

我们知道，假如环 R 是理想 R_i 的直和，即 $R=R_1+\cdots+R_m$，如果 R 是阿丁环，因为 R_i 的左理想也是 R 的左理想，所以 R_i 也是阿丁环，这就是说，假如 R 是阿丁环，那么它的直和因子也是阿丁环，反过来也成立.

定理 3 假定环 R 是理想 R_1,R_2 的直和，即 $R=R_1+R_2$，如果 R_1,R_2 都是阿丁环，那么 R 也是阿丁环.

证明 由环的第二同态定理，我们得知 $R_2\simeq R-R_1$，所以 $\bar{R}=R-R_1$ 满足极小条件，这就是说，$R_1,\bar{R}$ 都是阿丁环，因此由上定理，R 是阿丁环. 证毕.

一般，假定环 $R=R_1+\cdots+R_n$，如果理想 $R_1,\cdots,R_n$ 都是阿丁环，那么 R 也是阿丁环.

同样，假如 R-模 M 是子模 M_1,M_2 的直和，即 $M\doteq M_1+M_2$，如果 M_1,M_2 都是阿丁模，同上定理的证明一样，M 也是阿丁模. 因此如果环 R 是它的左理想 R_1,R_2 的直和，R_1,R_2 又都是阿丁模，那么$_kR$ 也是阿丁模.

定理 4 假定 R 是阿丁环，那么全矩阵环 R_n 也是阿丁环.

证明 假设 RE_{ij}是 R_n 中所有 i 行 j 列上是 R 中元其余都是 R 中零元的 n 阶矩阵，那么 $R_n=\Sigma RE_{ij}$，因为 R,RE_{ij}看成 R-模时 $R\sim RE_{ij}$，而 R 是阿丁模，所以 RE_{ij}也是阿丁模，即 RE_{ij}的任意子模的降链序列只有穷项，同定理 3 一样，R_n 看成 R-模时，它的任意子模的降链序列也只有穷项. 再我们把 R 中元 a 看成 R_n 中对角形矩阵 $\mathrm{dig}(a,\cdots,a)$，那么 R 就是 R_n 的子环. 因此 R_n 的左理想显然是 R 的子模. 于是 R_n 的任意左理想列只有穷项，即 R_n 是阿丁环，所以定理成立.

特别，假如 K 是体，那么全矩阵环 K_n 是阿丁环. 这定理的逆也是成立的，即假如全矩阵环 R_n 是阿丁环，那么环 R 也是阿丁环，这是因为如果 R 不是阿丁环，左理想列

$$L_1\supset L_2\supset\cdots\supset L_m\supset\cdots$$

有无穷项，那么 R_n 的左理想列

$$(L_1)_n\supset(L_2)_n\supset\cdots\supset(L_m)_n\supset\cdots$$

也有无穷项，这显然与假设矛盾.

阿丁环具备很多重要性质. 下面是其中荦荦大者：

我们知道，元数是有穷的无零因子环是体（§3.2）. 一般我们有

定理 5 无零因子阿丁环是体.

证明 假定阿丁环 R 是无零因子环，a 是 R 中非零元，对于左理想列

$$Ra\supset Ra^2\supset\cdots,$$

根据极小条件，有整数 m，使 $Ra^m=Ra^{m+1}$，因此 $ba^m=ca^{m+1}$，但 $a^m\neq 0$，所以 $ca=b$，由 §3.2 定理 2，得 R 是体，所以定理成立.

我们知道，在交换环中质理想不一定是极大理想，但在阿丁环中却是如此，即

定理 6 在交换阿丁环中，质理想是极大理想.

证明 假定 P 是交换阿丁环 R 的质理想，那么 $\overline{R}=R-P$ 是整环，又因为 $\overline{R}$ 是阿丁环，由上定理，$\overline{R}$ 是域，因此 P 是极大理想，定理成立.

与不可分解群(§6.4)类似，有不可分解模. 环 R 的左理想是 $_RR$ 的不可分解模时，叫做 R 的**不可分解左理想**.

定理 7 假定 R 是阿丁环，那么 R 是有穷个不可分解左理想的直和.

证明 假定 M 是 R 中所有不能表为有穷个不可分解左理想直和的左理想的集合，如果 M 非空，根据极小条件，M 有极小左理想 L_0，显然 L_0 是可分解的. 设 $L_0=L_1+L_2$，因为 $L_1,L_2\subset L_0$，所以 $L_1,L_2\subseteq M$，于是 L_1,L_2 都能表为有穷个不可分解左理想的直和，因此 L_0 也能如此，这与 $L_0\subset M$ 的假设矛盾. 于是定理成立.

在上面的讨论中，假如把左理想换成右理想，我们就得到满足右理想极小条件的类似理论. 满足右理想极小条件的环叫做**右阿丁环**，因此前面阿丁环有时又叫做**左阿丁环**. 要注意一个左阿丁环不一定又是右阿丁环，即一个环，它满足左理想的极小条件不一定就满足右理想的极小条件. 譬如，假定 A 是基础体为有理数域 Q，底元为 e,a 的代数，即

$$A=Qe+Qa,$$

其中
$$e^2=e,a^2=0,ea=a,ae=0,$$

因为 A 的左理想是 A 的子空间，所以它满足左理想的极小条件. 假如(m)是 Q 中整数 m 的所有倍数形成的加群，因为 A 中任意元右乘$(m)a$ 都成为零，所以$(m)a$ 是 A 的右理想，因此 A 的右理想列

$$(m)a \supset (2m)a \supset (2^2m)a \supset \cdots$$

含有无穷项，所以 A 不满足右理想的极小条件. 这就是说 A 是左阿丁代数，但不是右阿丁代数.

习 题 8.1

1. 假定 V 是环 R 的既约模，x 是 V 中任意元，试证 $Rx=V$ 或 $Rx=0$.

2. 假定 V 是 R-模，并且 V 中任意非零元不能够被 R 中所有元零化，如果 V 是它的既约子模 $V_1,\cdots,V_m$ 的直和，同时又是既约子模 $W_1,\cdots,W_n$ 的直和，即 $V=V_1+\cdots+V_m=W_1+\cdots+W_n$，那么 $m=n$.

3. 假如 R 不满足极小条件，全矩阵环 R_n 是否也不满足极小条件?

§8.2 幂零理想

从§3.7我们知道，假定 L 是环 R 的左理想，如果其中任意元都是幂零元，就叫 L 做幂零元左理想，如果 L 的某乘幂是零理想，就存在某正整数 m，使

$$L^m=0,$$

那么 L 叫做幂零左理想. 显然，幂零左理想是幂零元左理想. 反过来不一定成立，即幂零元左理想不一定是幂零左理想. 即令环 R 中任意元 $a^n=0$，n 是固定的，我们也无法推得 $R^n=0$，因为这时要求 $a_1\cdots a_n=0$，$a_i\in R$. 这样的例子也是常见的.

在交换环中，两个幂零元的和仍然是幂零元. 在一般环中这性质不成立，因此，两个幂零元左理想的和不一定是幂零元左理想. 但对于幂零左理想，我们有：

定理 1 假定 L_1、L_2 是环 R 的幂零左理想，那么它们的和 (L_1,L_2) 也是 R 的幂零左理想.

证明 假定

$$L_1^{m_1}=0, L_2^{m_2}=0,$$

根据结合律及分配律，我们把 L_1,L_2 的和 (L_1,L_2) 的 m_1+m_2-1 乘

幂$(L_1,L_2)^{m_1+m_2-1}$展开，就成为每项含有 m_1+m_2-1 个因子的展开式，在这展开式的任意一项中，如果含 L_1 的个数小于 m_1，那么它含 L_2 的个数就不小于 m_2，因为 L_1,L_2 都是 R 的左理想子环，当它含 L_1 的个数不小于 m_1 时，我们就有

$$\cdots L_1\cdots L_1\cdots L_1\cdots\subseteq\cdots L_1^{m_1}\cdots=0,$$

当它含 L_2 的个数不小于 m_2 时，我们有

$$\cdots L_2\cdots L_2\cdots L_2\subseteq\cdots L_2^{m_2}\cdots=0,$$

这就是说，展开式中任意项都是零理想，所以$(L_1,L_2)^{m_1+m_2-1}=0$，于是定理成立.

因为左理想的和适合分配律，所以有穷个幂零左理想的和仍然是幂零左理想，但无穷个幂零左理想的和* 一般只能是幂零元左理想而不是幂零左理想. 这是因为，假如 a 是无穷个幂零左理想的和 L 中任意元，根据定义，a 是其中某有穷个幂零左理想的和中元，因此 a 是幂零元，但这些乘幂不一定有最大数，所以 L 不是幂零左理想.

在什么条件下幂零元左理想又是幂零左理想？1939 年霍布金斯(C. Hopkius，1902～1939)给出了一个定理[8]，下面是 1942 年提出要求更强的布劳尔定理[9].

定理 2 假定 R 是阿丁环，L 是 R 的左理想，如果 L 不是幂零左理想，那么 L 中有幂等元，因此 L 不是幂零元左理想.

证明 我们先在 L 中找出一个适当的非幂零元.

因为 R 满足极小条件，所以 L 中所有 R 的非幂零左理想集合有极小左理想，假定 L_1 是这极小左理想；因为 $L_1^2\subseteq L_1$，并且 L_1^2 又是 L 中 R 的非幂零左理想，所以 $L_1^2=L_1$. 再 L_1 中所有满足 $L_1L'\neq 0$ 的 R 的左理想 L' 的集合，由极小条件，它也有极小左理想 L_2，因此 $L_1L_2\neq0$. 于是在 L_2 中有元 u 使

$$L_1u\neq0$$

---

* 这里所谓的和指的是离散的直接和(§6.4).

又因为 L_1u 是 L_2 中 R 的左理想，并且 $L_1 \cdot L_1u = L_1u \neq 0$，所以 $L_1u = L_2$. 因此在 L_1 中有满足

$$eu = u$$

的元 e. 于是，对于任意正整数 n，我们有 $e^n u = u$，因为 $u \neq 0$，所以 e 不是幂零元. 这就是说，L_1 中有非幂零元 e.

再我们引用这非幂零元 e 来求幂等元.

我们容易知道，L_1 中所有满足 $xu = 0$ 的元 x 形成 R 的左理想 L_1'，因为 $e^2u = eu$，即 $(e^2 - e)u = 0$，所以 $e^2 - e \in L_1'$. 又因为 $L_1u \neq 0$，所以 $L_1' \subset L_1$，但 L_1 是 R 的非幂零极小左理想，因此 L_1' 是幂零左理想. 于是 $e^2 - e = t$ 是幂零元. 我们命 $t^n = 0$，如果 $n = 1$，那么 $e^2 = e$，即 e 是幂等元. 所以这时定理成立，如果 $n \neq 1$，命

$$e_1 = e - 2et + t,$$

显然 e_1 不是幂零元，由计算我们容易得知

$$e_1^2 = e_1 + 4t^3 - 3t^2, \text{即 } e_1^2 - e_1 = 4t^3 - 3t^2.$$

因此 $e_1^2 - e_1 = t_1$ 又是幂零元，命 $t_1^{n_1} = 0$，显然 $n > n_1$. 如果 $n_1 = 1$，那么 $e_1^2 = e_1$，即 e_1 是幂等元. 所以这时定理成立. 如果 $n_1 \neq 1$，命

$$e_2 = e_1 - 2e_1t_1 + t_1, e_2^2 - e_2 = t_2$$

重复引用上面方法，我们就得到幂零元列 $t, t_1, t_2, \cdots$；因为它们的乘幂 $n > n_1 > n_2 > \cdots$，所以最后得 $n_m = 1$. 于是 $t_m = e_m^2 - e_m = 0$，即 e_m 是幂等元. 因此定理成立.

于是我们得下面重要的**霍布金斯定理**

定理 3 在阿丁环中，幂零元左理想是幂零左理想.

在阿丁环中，所有幂零左理想的和仍然是幂零左理想. 这是因为任意元是其中某有穷个幂零左理想中元的和. 这最大的幂零左理想在讨论环的构造时起着重大的作用，因此我们有

定义 假定 R 是阿丁环，那么 R 中所有幂零左理想的和是 R 中最大幂零左理想，叫做 R 的**根基**. 用 $N(R)$ 或 N 表示.

要注意的是，阿丁环 R 的根基 N 中元都是幂零元，但 R 的幂零元不一定都在 N 中. 譬如全矩阵环 Q_2 的根基是零（§8.4 定理

6)，但$\begin{pmatrix}0&1\\0&0\end{pmatrix}$，$\begin{pmatrix}0&0\\1&0\end{pmatrix}$都是幂零元.

假如 R 又是交换环，a 是 R 的幂零元，那么 ra，$r\in R$ 也是幂零元，因此，由 a 生成的理想是幂零理想，所以 $a\in N$. 于是 N 是 R 中所有幂零元组成的理想.

定理 4 假定 R 是阿丁环，N 是其根基，那么 R 中元 $a\in N$ 的必要充分条件是 ra 都是幂零元，这里 r 是 R 中任意元.

证明 假如 $a\in N$，那么 $ra\in N$，因此 ra 是幂零元. 反过来，如果 ra 都是幂零元，因为

$$(ra+na)^2=\{(ra+na)r+n(ra+ua)\}a=r'a$$

所以 $ra+na$ 是幂零元，因此，由 a 生成的左理想 L 是幂零元理想，于是 $L\subseteq N$，所以 $a\in N$. 因此定理成立.

下面是根基的两个基本性质.

定理 5 环 R 的根基 N 是 R 的幂零理想，它既包含 R 的所有幂零左理想，也包含 R 的所有幂零右理想.

证明 因为 N 是 R 的幂零左理想，假定 $N^m=0$，那么 $(NR)^m=N\cdot RN\cdots RN\cdot R\subseteq N^mR=0$，即 NR 是 R 的幂零理想，因此 $NR\subseteq N$，这就是说，N 是 R 的理想.

再假定 K 是 R 的幂零右理想，我们可以同样证明 RK 是 R 的幂零理想，因此它们的和 (K,RK) 也是 R 的幂零理想，于是 $(K,RK)\subseteq N$，所以 $K\subseteq N$，即 N 包含 R 的所有幂零右理想. 因此定理成立.

一个阿丁环，如果它的根基是零，就叫做半单纯环或半单环；如果它的根基是自身，就叫做根基环. 显然阿丁幂零环是根基环，当然，根基环也是幂零环. 不含非零的幂零左理想的阿丁环是半单环. 因为幂等元不是幂零元，所以有幂等元的阿丁环不是根基环. 假如 R 是交换阿丁环，如果 R 有非零的幂零元，那么 R 不是半单环.

定理 6 假定 N 是环 R 的根基，那么 $\bar{R}=R-N$ 的根基是零，

也就是说，$\bar{R}$ 是半单环.

证明 因为 R 是阿丁环，由§8.1定理1，$\bar{R}$ 也是阿丁环. 再假定 $\bar{L}$ 是 $\bar{R}$ 的幂零左理想，$\bar{L}^m=\bar{0}$，L 是 $\bar{L}$ 在 R 的完全象源，那么 $L^m\equiv 0(N)$，即 $L^m\subseteq N$. 但 N 是 R 的幂零理想，$N^n=0$，于是 $L^{mn}=0$，因此 L 是 R 的幂零左理想，所以 $L\subseteq N$，即 $\bar{L}=\bar{0}$，这就是说，$\bar{R}$ 中只有零理想是幂零左理想，因此 $\bar{R}$ 的根基是零，所以 $\bar{R}$ 是半单环，于是定理成立.

定理7 环 R 的根基 N 既包含 R 的所有幂零元左理想，也包含 R 的幂零元右理想.

证明 因为 R 的幂零元左理想是幂零左理想，所以它在根基 N 中.

再假定 K 是 R 的幂零元右理想子环，$\bar{K}$ 是 K 在 $\bar{R}=R-N$ 的象，如果能够证明 $\bar{K}=\bar{0}$，那就有 $K\subseteq N$. 设 $\bar{x}\in\bar{K}$，因为 $\bar{R}\bar{x}$ 是 $\bar{R}$ 的幂零元左理想，所以 $\bar{R}\bar{x}=\bar{0}$，于是 $\bar{R}\bar{K}=\bar{0}$，因此 $\bar{K}$ 是 $\bar{R}$ 的幂零元左理想，所以 $\bar{K}=\bar{0}$. 定理证毕.

于是，在(左)阿丁环 R 中，幂零元左理想当然是幂零，幂零元右理想也同样是幂零. 因此，这时幂零元与幂零是一致的. 再 R 的最大幂零左理想与最大幂零右理想一致. 因此 R 的根基也可用幂零右理想来建立.

我们知道，阿丁环的子环不一定也是阿丁环，就是阿丁环，子环的根基与环的根基的关系也不清楚，假如子环是理想并且又是阿丁环，我们就有下面关系.

定理8 假定 R 是阿丁环，N 是它的根基，R_1 是 R 的理想并且又是阿丁环，N_1 是 R_1 的根基，那么

$$N_1=R_1\cap N$$

证明 因为 $R_1\cap N$ 是 R_1 的理想，并且又是幂零，所以 $R_1\cap N\subseteq N_1$. 再假定 $a\in N_1$，那么 $a,r_1a\in N_1$，即 a,r_1a 都是幂零元，又因为 $a\in R_1$，所以 $rar\in R_1$. 这里 $r\in R$，于是 $(ra)^2=(rar)a=r_1a$，所以 $(ra)^2$ 是幂零元，即 ra 是幂零元，因此 $a\in N$，所以 $N_1\subseteq R_1\cap N$.

定理证毕.

于是,假如 R_1 是阿丁环 R 的理想,如果 R_1 又是 R 的直和因子,那么 R_1 的根基 $N_1=R_1\cap N$,这里 N 是 R 的根基.

习 题 8.2

1. 试求 3 次代数 $A=Fu_1+Fu_2+Fu_3$ 的根基,A 的乘法表是

	u_1	u_2	u_3
u_1	u_1	0	u_3
u_2	0	u_2	0
u_3	0	u_3	0

2. 试证同余环 $Z-(m)$ 的根基是零的必要充分条件为:m 不能用质数的平方整除.

3. 试证根基是零的环,它的中心的根基也是零.

4. 假定 N 是环 R 的根基,M 是 R 的理想,那么 $\bar{R}=R-M$ 的根基是 $(M,N)-M$.

5. 在任意环中,任意幂零左理想能够嵌入幂零理想.

6. 假如 L 是环 R 的极小左理想,试证 $L^2=0$ 或 $L=Re$,这里 e 是幂等元.

7. 假定 N 是环 R 的理想,如果 $N,\bar{R}=R-N$ 都是幂零,那么 R 也是幂零.

8. 假定环 R 是子环 R_1,R_2 的直和,即 $R=R_1+R_2$,R 是阿丁环,N,N_1,N_2 分别是 R,R_1,R_2 的根基,试证 $N=N_1+N_2$.

§8.3 半 单 环

有了上面两节的知识,我们就容易把魏特邦定理推广,这节我们主要是讨论半单环的构造.

下面,先讨论半单环的左理想及理想.我们知道,假如 a 是环 R 中任意元,那么 Ra 是 R 的左理想.当 R 是半单环时,它的逆也

基本成立，即

定理1 半单环R的任意非零左理想L含有幂等元e，并且$L=Re$.

证明 首先因为R的根基是零，所以L不是幂零，由§8.2定理2，L含有幂等元e.

再L中所有满足$xe=0$的元x形成R的左理想，我们用L_e表示. 因为L中幂等元可能不只一个，因此所有这样的左理想也可能不只一个. 但R满足极小条件，所以所有这样的左理想集合有极小左理想，我们假定这极小左理想就是L_e，也就是说，上面的幂等元e我们是如此选择的.

假如$L_e=0$，设x是L中任意元，因为$(x-xe)e=0$，所以$x-xe\in L_e$. 因此$x=xe$. 于是$L=Le$，即e是L的右单位元，又因为$Le\subseteq Re\subseteq L$，所以$L=Re$. 定理就成立.

假如$L_e\neq 0$，那么它含有幂等元e_1，显然$e_1e=0$. 命$e'=e-ee_1+e_1$，由计算我们容易得知，$e'e'=e'$，$e'e=e\neq 0$，所以$e'\neq 0$，因此e'是幂等元. 于是我们有左理想$L_{e'}$. 再因为$e'e=e$，所以当$xe'=0$时$xe=0$，又因为$e_1e'=e_1\neq 0$，所以$Le'\subset L_e$，这与L_e是极小的假设矛盾. 于是$L_e=0$.

定理证毕.

定理2 半单环R中非零理想$N=Re=eR$，这里幂等元e由N唯一决定，并且e在R的中心$Z(R)$中.

证明 因为N也是R的左理想，所以$N=Re$. 再N中所有满足$ex=0$的元x形成R的右理想M，显然$Me=M$，$eM=0$. 于是$M^2=MeM=0$，因此M是R的幂零右理想. 但R的根基是零，所以$M=0$. 于是对于N中任意元x，由$e(x-ex)=0$，我们就有$x-ex=0$，所以$N=eN=eR$. 因此$N=Re=eR$，因为e是N的单位元，所以是唯一的，

再如果x是R中任意元，因为

$$ex=ex\cdot e=e\cdot xe=xe,$$

所以 e 在 $Z(R)$ 中，于是定理成立.

假如 e 是半单环 R 的幂等元，如果 e 在 $Z(R)$ 中，显然 e 是 R 的理想 $N=Re=eR$ 的单位元. 因此，R 的幂等元是它的理想的单位元的必要充分条件是它在 R 的中心 $Z(R)$ 中. 因为环自身也是理想，所以半单环有单位元.

于是半单环的左理想是由其中幂等元生成的. 1946 年，柯德曼(O. Goldman)证明了它的逆，即环的任意左理想如果都是由幂等元生成的，那么这环是半单环[10].

定理 3 半单环的理想是半单环.

证明 假定 L 是半单环 R 中理想 $N=Re=eR$ 的左理想，因为 $L\subseteq N$；所以 $L=eL$，因此 $RL=ReL\subseteq NL\subseteq L$，所以 L 也是 R 的左理想. 因为 R 满足极小条件，所以 N 也满足极小条件. 又因为 R 中没有非零的幂零左理想，所以 N 也没有非零的幂零左理想. 因此 N 的根基是零，于是定理成立.

因为半单环的理想有单位元，由 §6.4 定理 7 即得

定理 4 假定 $N=Re=eR$ 是半单环 R 的理想，那么 N 是 R 的直和因子，即

$$R=N+N',$$

这里 N' 是 R 的理想，并且由 N 唯一决定.

我们也可以简证 N 是直和因子如下. 假定 r 是 R 中任意元，因为

$$r=re+r-re$$

所以 $R=(N,N')$，这里 $N'=\{r-re|r\in R\}$，因为 $e\in Z(R)$，所以 N' 是 R 的理想. 又因为 $Ne=N$，$N'e=0$，所以 $N\cap N'=0$. 于是 R 是理想 N，N' 的直和，即 $R=N+N'$.

现在我们来讨论半单环的构造.

我们知道，一个环如果除自身及零理想外没有其他理想，就叫做单环. 环 R 的理想如果又是单环，就叫做 R 的单理想.

假定 $R\neq 0$ 是阿丁单环，N 是它的根基；因为 R^2 是 R 的理想，

所以$R^2=R$或$R^2=0$. 又因为N是R的理想，所以$N=0$或$N=R$，但N是幂零，所以当$R^2=R$时，$N=0$；当$R^2=0$时，$N=R$. 这就是说当$R^2=R$时，R是半单环；当$R^2=0$时R是根基环，即阿丁单环非幂零时是半单环，幂零单环时是根基环.

下面是半单环的构造定理，这定理又叫**魏特邦-阿丁第一构造定理**.

定理 5 半单环R只有有穷个单理想，R是它的所有单理想的直和，并且R的任意理想是包含在其中R的所有单理想的直和.

证明 因为R的理想N仍然是半单环，并且N的理想又是R的理想，因此只要证明定理的前半段，后半段就是显然的了.

由定理4，根据极小条件我们容易得知，R中所有非零理想集合的极小理想是R的单理想，这就是说，R含有单理想. 假定N_1是R的单理想，由定理4，我们有

$$R=N_1+N'_1,$$

这里N'_1是R的理想. 如果$N'_1\neq 0$又不是单理想，那么N'_1含有R的单理想N_2，于是我们有$N'_1=N_2+N'_2$，因此

$$R=N_1+N_2+N'_2.$$

如果$N'_2\neq 0$又不是R的单理想，我们又可继续分解. 因为R满足极小条件，所以R的理想列

$$R\supset N'_1\supset N'_2\supset\cdots$$

只能有穷项，因此有整数n，使$N'_n=0$. 于是

$$R=N_1+N_2+\cdots+N_n,$$

这就是说，R是n个单理想的直和.

假如我们能够证明R的任意有穷个单理想的和都是直和，那么R就只有n个单理想，因此R就是它的所有单理想的直和，定理就告成立.

假定$N_i=Re_i=e_iR$，$i=1,\cdots,m$，是R的m个单理想，因为$N_i\cap N_j$，$i\neq j$，是N_i的理想，所以$N_i\cap N_j=0$，因此$N_iN_j=0$. 于是

$e_iN_j=0$. 如果

$$a_1+\cdots+a_m=0, a_i\in N_i,$$

那么
$$e_ia_i=a_i=0.$$

因此$(N_1,\cdots,N_m)$中任意元能够唯一地表为$N_1,\cdots,N_m$中元的和，所以$(N_1,\cdots,N_m)=N_1+\cdots+N_m$，定理成立.

于是，半单环的构造由它的所有单理想的构造完全决定，因此，半单环的构造问题可以归结为单环的构造问题了. 下节，我们还要详细讨论单环的构造.

由§3.6定理3，我们得知非幂零的交换单环是域，因此，由定理5，我们即得下面的德狄亭得定理.

定理6 元数大于1的交换半单环是有穷个域的直和.

下面是定理5的逆.

定理7 假定R是阿丁单环$R_1,\cdots,R_n(R_i^2\neq 0)$的直和，即$R=R_1+\cdots+R_n$，那么$R$是半单环.

证明 根据假设，R_i是阿丁环，由§7.1定理3，我们得知，R也是阿丁环.

再因为$R_i^2\neq 0$，所以R_i又是半单环，因此它有单位元，于是R是有单位元的环. 假定L是R的幂零左理想，$L^m=0$，由§6.4定理8我们有

$$L=L_1+\cdots+L_n, L_i=L\cap R_i,$$

因此
$$L^m=L_1^m+\cdots+L_n^m.$$

所以$L_i^m=0$，即L_i是R_i的幂零左理想，但R_i是半单环，所以$L_i=0$，于是$L=0$. 这就是说，R的根基是零. 于是R是半单环，因此定理得证.

最后是单环的基本性质.

假如R是幂零单环，那么$R^2=0$，因此R中任意两元的乘积都是零. 同§3.6定理1一样，R的元数是质数. 于是我们有

定理8 幂零单环是根基环，它的元数是质数.

以后，我们所说的单环指的都不是幂零单环. 于是阿丁单环是

半单环，因此它也有单位元，即阿丁单环也有单位元. 但要注意，不是任意单环都有单位元.

下面是单环与定理4类似的性质.

假如把定理4中R改为单环，N改为R的左理想，定理仍然成立，这时N'是R的左理想，但不一定是由N唯一决定的，再根据定理5的证明，我们即得

定理9　阿丁单环是有穷个极小左理想的直和.

要注意的是，这里的直和不是环的直和而是把R看成R-模的直和，半单环分解为单理想的直和是唯一的，单环分解为极小左理想的直和不是唯一的. 但我们不难证明它的直和因子的个数是一致的（§8.1 习题2），也就是说，单环的直和因子的个数由它自身唯一决定，这个数有时又叫做单环的长. 譬如，全矩阵环Q_2可以分解为$Q_2E_1+Q_2E_2$，也可以分解为$Q_2E_1+Q_2E_3$，即

$$Q_2=Q_2E_1+Q_2E_2,\quad Q_2=Q_2E_1+Q_2E_3,$$

这里
$$E_1=\begin{pmatrix}1&0\\1&0\end{pmatrix},\quad E_2=\begin{pmatrix}0&1\\0&1\end{pmatrix},\quad E_3=\begin{pmatrix}2&2\\-1&-1\end{pmatrix}.$$

Q_2的长显然是2.

于是，半单环是有穷个极小左理想的直和.

定理10　阿丁单环的极小左理想相互同构.

证明　假定L_1,L_2是单环R的极小左理想，因为单环是半单环，所以$L_1=RL_1,L_2=RL_2$. 如果$L_1L_2=0$，由$L_2=RL_2$，我们就有$L_1RL_2=0$，因此$L_1RL_2R=0$. 但L_1R,L_2R都是R的非零理想，而R是单环，所以$L_1R=R,L_2R=R$. 于是$R^2=0$，这与我们的假设不合，因此$L_1L_2\neq0$. 于是在L_2中有元a使$L_1a\neq0$，但$L_1a\subseteq L_2$而L_2是极小左理想，所以$L_2=L_1a$. 显然$x\to xa$是L_1到L_2上的同态（R-模同态）. 因为L_1是极小左理想，所以这同态又是同构. 于是$L_1\simeq L_2$，因此定理成立.

定理11　半单环的极小左理想如果包含在同一单纯理想中，它们就同构；如果不包含在同一单理想中，它们就不同构.

证明 假定L_1, L_2是半单环R的极小左理想，如果L_1, L_2同在R的一个单理想中，由上面定理10，$L_1 \simeq L_2$. 如果L_1, L_2分别在不同的单理想N_1, N_2中，因为N_1, N_2是R的直和因子，所以$N_1N_2=0$，命e_1是N_1的单位元，$e_1L_1=L_1$，$e_1L_2=0$，所以L_1, L_2看成R-模时不同构，因此定理成立.

定理 12 假定L是任意环R的左理想，那么R中所有与L同态的左理想的和是R的理想.

证明 R中所有与L同态的左理想的和N显然是R的左理想. 假定a是R中任意元，L'是R中与L同态的任意左理想，那么$L'a$又是R的左理想. 因为$x \to xa$是L'与$L'a$的同态，所以$L' \sim L'a$，因此$L \sim L'a$，于是$L'a \in N$，因此$NR \subseteq N$，这就是说，N是R的理想，所以定理得证.

再要注意的是，上面的同态、同构都是R-模的同态、同构，而不是环的同态、同构.

于是我们得知，半单环R假如先分解为单理想的直和，再把各个单理想分解为极小左理想的和，我们就得到R分解为极小左理想的直和. 假如先分解为极小左理想的直和，再我们不难证明其中所有相互同构的极小左理想的和是R的单理想，这样我们就得到R分解为单理想的直和.

习 题 8.3

1. 半单环的中心是域的直和.

2. 一个幂等元，如果不能写成两个正交幂等元的和，就叫做本原幂等元. 试证e是本原幂等元的必要充分条件是对于任意幂等元f，从$f=ef=fe$，即得$e=f$.

3. 试证半单环R的左理想$L=Re$是极小的必要充分条件为e是本原幂等元. 因此R的极小左理想是不可分解左理想.

4. 假定环R有单位元并且是有穷个极小左理想的直和，那么R是半单环.

§8.4 单 环

上节讨论了半单环的构造，现在讨论满足极小条件的单环的构造即阿丁单环的构造.

下面是(非幂零)单环的构造定理，这定理又叫做魏特邦-阿丁第二构造定理，这节主要是证明这定理.

定理 1 单环 $R(R^2\neq 0)$ 与全矩阵环 K_n 同构，并且整数 n 及体 K(除同构外)由 R 唯一决定，这 K 叫做 R 所属的体.

这定理就是说 R 中元可以用矩阵来表示. 在线代数中曾证明，向量空间的线性变换可以用矩阵表示. 这里与它类似，证明方法基本上一样. 我们首先要求建立一个体 K 的有穷维向量空间，R 中元是这向量空间的线性变换，再求出与 R 中元对应的矩阵，然后根据同构定义，证明 R 与这些矩阵组成的全矩阵环同构，于是证明完毕. 下面，就是根据这个步骤来逐步完成.

首先我们来建立体 K，这样我们有

定理 2 假定环 R(不要求是阿丁环)不含非零的幂零左理想，e 是 R 的幂等元，那么左理想 $L=Re$ 是 R 的极小左理想的必要充分条件是：eRe 是体.

证明 假定 $L=Re$ 是 R 的极小左理想，我们来证明 eRe 是体. 我们容易知道 eRe 是环，这是因为，形如 ere，$r\in R$，的元其和、差、积仍然是这样形状的元. 又因为 e 是幂等元，所以 e 是 eRe 的单位元. 再假定 $ere\neq 0$，那么 $Rere$ 是 L 中 R 的非零左理想，因为 L 是极小左理想，所以 $Rere=Re$，于是

$$eRe\cdot ere=eRe$$

这就是说，方程 $xa=b$ 在 eRe 中有解，因此 eRe 成体.

反过来，假如 eRe 是体，我们来证明 $L=Re$ 是 R 的极小左理想. 假定 $L'\neq 0$ 是 L 中 R 的左理想，如果 $eL'=0$，那么

$$L'L'\subseteq LL'\subseteq ReL'=0,$$

这与 R 中没有非零的幂零左理想的假设不合，因此 $eL'\neq 0$. 于是 $eL'=eL'e$ 是体 eRe 的非零左理想，所以 $eRe=eL'$，因此 $e\in eL'\subseteq L'$，所以

$$L=Re\subseteq RL'\subseteq L',$$

于是 $L=L'$，这就是说，L 是 R 的极小左理想，因此定理成立.

假如把上定理中左理想换成右理想，显然定理仍然成立. 这就是说，假如环 R 不含非零的幂零右理想，那么 $M=eR$ 是 R 的极小右理想的必要充分条件是：eRe 成体. 因此，假如环 R 不含非零的幂零左理想，也不含非零的幂零右理想，如果 Re 是 R 的极小左理想，那么 eR 就是 R 的极小右理想. 反过来，如果 eR 是 R 的极小右理想，那么 Re 就是 R 的极小左理想. 于是，假如 R 是单环，如果 Re 是极小左理想，那么 eR 就是极小右理想，反过来也成立.

这样，我们得到体 $K=eRe$. 再我们来建立 K 的有穷维向量空间.

假定 R 是单环，$L=Re$ 是 R 的极小左理想，$K=eRe$. 命 $V=eR$，因为

$$KV=eRe\cdot eR\subseteq eR=V,$$

所以 V 是体 K 空间. 下面我们来讨论 V 的维数.

假定 $u_1,\cdots,u_n$ 是 V 中关于 K 线性无关的元，因为 $eu_i=u_i\neq 0$，所以 $Lu_i\neq 0$. 又因为 L,Lu_i 看成 R-模时是同构的，所以 Lu_i 是 R 的极小左理想. 假如我们能够证明 $Lu_1,\cdots,Lu_n$ 的和 $(Lu_1,\cdots,Lu_n)$ 是直和，那么 V 关于 K 的维数就不大于 R 的长，于是 V 关于 K 的维数是有穷. 再假如 V 关于 K 的维数是 n，命 $V=Ku_1+\cdots+Ku_n$，因为 $LV=ReR$ 是 R 的理想，所以 $R=LV$. 又因为 $LK=Re\cdot eRe\subseteq L$，而 LK 是 R 的左理想，所以 $LK=L$. 于是 $R=(Lu_1,\cdots,Lu_n)$，这就是说，R 的长不大于 V 的维数. 因此，只要我们能够证明

$$(1)\qquad (Lu_1,\cdots,Lu_n)=Lu_1+\cdots+Lu_n,$$

那么 V 关于 K 的维数就是 R 的长了.

要证明(1)，只要证明

$$a_1u_1+\cdots+a_nu_n=0, a_i\in L$$

时，$a_iu_i=0, i=1,\cdots,n$. 我们用反证法来证明，假定 a_iu_i 不完全都是零，譬如 $a_1u_1\neq 0$，那么 $a_1u_1\in(Lu_2,\cdots,Lu_n)$，因此左理想$(Lu_2,\cdots Lu_n)$与极小左理想 Lu_1 的交集异于零，于是

$$Lu_1\subseteq(Lu_2,\cdots,Lu_n).$$

因此，我们有 $eu_1+a_2'u_2+\cdots+a_2'u_n=0, a_i'\in L$，即

$$eu_1+ea_2'u_2+\cdots+ea_n'u_n=0.$$

但 e, ea_i' 都是 K 中元而 $e\neq 0$，这与 $u_1,\cdots,u_n$ 关于 K 线性无关的假设不合，所以(1)成立.

于是我们有

定理 3 假定 R 是单环，它的长是 n，$L=Re$ 是 R 的极小左理想，$K=eRe$，那么 $V=eR$ 是 n 维 K 向量空间.

由上面的证明我们还知道，假如 $u_1,\cdots,u_n$ 是 V 关于 K 的底，即 $V=Ku_1+\cdots+Ku_n$，那么 R 就是极小左理想 $Lu_1,\cdots,Lu_n$ 的直和，即 $R=Lu_1+\cdots+Lu_n$.

有了 K 空间 V 后，我们就容易求得与 R 中元对应的矩阵了.

假定 $V=Ku_1+\cdots+Ku_n$，因为 V 是 R 的右理想，所以对于 R 中元 a，我们有

$$u_ia=a_{i1}u_1+\cdots+a_{in}u_n, a_{ij}\in K,$$

因此

$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}a=\begin{pmatrix}u_1a\\ \vdots\\ u_na\end{pmatrix}=A_a\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}, A_a=(a_{ij}).$$

即对于元 a 我们有矩阵 A_a. 同样对于 R 中元 b，我们有

$$\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}b=A_b\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}, A_b=(b_{ij}).$$

于是

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}(a+b)=A_{a+b}\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix},$$

但

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}(a+b)=\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}a+\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}b=(A_a+A_b)\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix},$$

所以

$$A_{a+b}\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}=(A_a+A_b)\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix},$$

因为 $u_1,\cdots,u_n$ 关于 K 线性无关，所以

$$A_{a+b}=A_a+A_b,$$

同样我们有

$$A_{ab}=A_a\cdot A_b.$$

于是映射 $a\to A_a$ 是 R 到 K_n 的同态. 根据下面定理 4，这映射是 R 到 K_n 的双射. 所以它是同构. 这就是说 R 与 K_n 同构. 因此定理 1 的前段成立.

定理 4 假定 $v_1,\cdots,v_n$ 是单环 R 的极小右理想

$$V=eR=Ku_1+\cdots+Ku_n$$

中任意 n 个元，那么 R 中有一且只有一个满足

$$v_i=u_ir,i=1,\cdots,n$$

的元 r.

证明 我们先证明 r 的唯一性. 假定 $u_ir=u_ir',i=1,\cdots,n$，那么 $u_i(r-r')=0$，但 R 中所有适合

$$u_ix=0,i=1,\cdots,n,$$

也就是使 $Vx=0$ 的元 x 组成 R 的右理想 N，因为 V 是 R 的右理想，所以 N 又是 R 的左理想. 于是 N 是 R 的理想，因此 $N=0$ 或

$N=R$，但$VR=V\neq 0$，所以$N=0$，这就是说，只有$x=0$适合上式，因此$r=r'$.

再我们来证明r的存在性. 我们容易知道，假如能够找到适合

$$u_i r_i = v_i, u_j r_i = 0, j\neq i, i=1,\cdots,n$$

的元r_i，那么$r_1+\cdots+r_n$就是所求的r，即$r=r_1+\cdots+r_n$. 下面我们来讨论如何找这样的r_i.

我们先求r_1. 假定$L'=Lu_2+\cdots+Lu_n$，因为L'是R的左理想，所以我们把它写成$L'=Re'$，这里e'是幂等元，并且$e'\neq 1$. 再因为

$$L'(1-e')=Re'(1-e')=R(e'-e')=0,$$

故$u_i(1-e')=0, i=2,\cdots,n$. 但$R=Lu_1+\cdots+Lu_n$，如果$u_1(1-e')$等于0，那么$R(1-e')$等于0，于是$1\cdot(1-e')=1-e'=0$，这与$e'\neq 1$的假设不合，所以$u_1(1-e')\neq 0$. 于是$u_1(1-e')R$是$R$的非零右理想. 因为$u_1\in V$，所以$u_1(1-e')R\subseteq V$，又因为$V$是$R$的极小右理想，所以$u_1(1-e')R=V$. 因此在$R$中有满足

$$u_1(1-e')r_1'=v_1.$$

的元r_1'，显然这时

$$u_i(1-e')r_1'=0, i=2,\cdots,n,$$

所以$(1-e')r_1'$就是所求的r_1，即$r_1=(1-e')r_1'$. 同样我们可以求得$r_2,\cdots,r_n$，这就证明了$r_1,\cdots,r_n$的存在性. 于是定理成立.

定理1中尚未证明的只是唯一性. 即，如果单环$R\simeq K_n$，那么整数n由R唯一决定，体K除同构外也由R唯一决定. 最后我们解答这问题.

首先我们知道，全矩阵环K_n可以写成n个极小左理想的直和，所以K_n的长是n，因此n就是R的长，所以n由R唯一决定.

再因为$R\simeq K_n$，命e是R中与K_n中元e'对应的元：

$$e\to e'=\begin{pmatrix}1 & \\ & 0\end{pmatrix},$$

那么e是幂等元，并且对于R中任意元r，

$$ere \to \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} \begin{pmatrix} k_{11} \cdots k_{1n} \\ \cdots \cdots \cdots \\ k_{n1} \cdots k_{nn} \end{pmatrix} \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} = \begin{pmatrix} k_{11} & \\ & 0 \end{pmatrix}.$$

因为这映射是 R 与 K_n 的同构，所以 $eRe \simeq K$，根据下定理，eRe 与 R 的极小左理想 $L=Re$ 的自同态环逆同构，但 R 的极小左理想相互同构，因此它们的自同态环也相互同构，这样，eRe 就是由 R 唯一决定的体了. 所以 K 除同构外由 R 唯一决定. 于是定理 1 中唯一性就完全得证.

定理 5 假定 $L=Re$ 是环 R 的左理想，那么 L 的自同态环 S 是 eRe 的逆环.

证明 假定 σ 是 $L=Re$ 的自同态，$\sigma(e)=a$，$a\in L$，那么对于 L 中任意元 re，$r\in R$，

$$\sigma(re)=r\sigma(e)=ra,$$

因此 re 的象由 e 的象 a 唯一决定，所以，我们又把 σ 写成 σ_a. 即 $\sigma_a(e)=a$，又因为

$$a=ae=\sigma(e)=\sigma(ee)=e\sigma(e)=eae,$$

即 $a=eae$，所以 $a\in eRe$. 这就是说，L 的任意同态 σ_a 由 eRe 中元 a 唯一决定. 反过来，假如 a 是 eRe 中任意元，显然映射

$$e\to ae, re\to ra, r\in R,$$

就是 L 的自同态 σ_a.

命 $\sigma_a\to a$，那么这映射是 L 的自同态环 S 到 eRe 的双射，再我们容易得知

$$(\sigma_a+\sigma_b)e=\sigma_a(e)+\sigma_b(e)=(a+b)e=\sigma_{a+b}(e),$$

$$\sigma_a\sigma_b(e)=\sigma_a\{\sigma_b(e)\}=\sigma_a(be)=b\sigma_a(e)=bae=\sigma_{ba}(e),$$

所以

$$\sigma_a+\sigma_b=\sigma_{a+b}, \sigma_a\sigma_b=\sigma_{ba}.$$

于是 $\sigma_a\to a$ 是 S 到 eRe 上的逆同构，因此 S 是 eRe 的逆环. 所以定理成立.

于是，上面的定理 1 完全得证.

由上面的证明，我们得知 R 包含它的所属体 $K=eRe$. 又假如 a 是 R 的中心中任意元，因为 $ae=ae^2=eae\in K$，所以由

$$u_ia=eu_ia=eau_i=aeu_i,$$

我们就得到

$$A_a=\begin{pmatrix} ae & & \\ & \ddots & \\ & & ae \end{pmatrix}=a\begin{pmatrix} e & & \\ & \ddots & \\ & & e \end{pmatrix}=aE, E=\begin{pmatrix} e & & \\ & \ddots & \\ & & e \end{pmatrix}.$$

这就是说，上面的同构把 R 的中心中元 a 变为 K_n 中元 aE，因为同构把中心变为中心，所以 K_n 的中心是 $Z(R)E$. 这结果也可由 §3.1 习题 9 推得.

下面是定理 1 的逆.

定理 6 假定 K 是体，那么全矩阵环 K_n 是单环.

证明 由 §7.1 定理 4，K_n 满足极小条件. 显然它不是幂零环.

再假定 N 是 K_n 中任意非零的理想，a 是 N 中非零元，E_{ij}是 n 阶矩阵，其中 i 行 j 列是 K 的单位元 1，其余都是零元 0，于是

$$a=\Sigma a_{ij}E_{ij}, a_{ij}\in K,$$

因为 $a\neq 0$，所以 a_{ij}不完全是 0. 假定 $a_{rs}\neq 0$，根据

$$\begin{aligned} E_{ij}E_{kl}&=0\ (j\neq k),\\ &=E_{il}(j=k), \end{aligned}$$

对于 K 中任意元 b，我们有

$$ba_{rs}^{-1}E_{ir}aE_{sj}=bE_{ij}\in N,$$

因此 $K_n\subseteq N$，所以 $N=K_n$，这就是说，K_n 中任意非零的理想只有单位理想，所以 K_n 是单环. 于是定理得证.

显然

$$L_i=KE_{1i}+\cdots+KE_{ni}, K_j=KE_{j1}+\cdots+KE_{jn}$$

分别是 K_n 的极小左理想及极小右理想，这里 $i,j=1,\cdots,n$.

因为 K_n 是左阿丁环也是右阿丁环，所以左单环也是右单环. 再左半单环也是右半单环，这是因为假如 R 是左半单环，由魏特

邦-阿丁第一构造定理，R 是有穷个左单环的直和，因此也是有穷个右单环的直和，由§8.3 定理 7，R 是右半单环.

习　题　8.4

1. 试证有穷非幂零单环是它的中心上的全矩阵环.

2. 试证 n 维 K 向量空间的自同态环与全矩阵环同构.

3. 半单环是单环的必要充分条件是它的中心是体.

4. 假如 e 是单环 R 的幂等元，试证 eRe 是体的必要充分条件是 e 是本原幂等元.

5. 假如 K 是体，试证全矩阵环 K_n 是极小左理想

$$L_i = KE_{1i} + \cdots + KE_{ni}, i=1, \cdots, n,$$

的直和，即

$$K_n = L_1 + \cdots + L_n.$$

并且 K_n 又是极小右理想 $R_i = KE_{i1} + \cdots + KE_{in}, i=1, \cdots, n$，的直和，即

$$K_n = R_1 + \cdots + R_n.$$

§8.5　贾柯勃逊根基

前面我们讨论了阿丁环的构造，此后三节讨论一般环的构造. 我们先从贾柯勃逊根基开始.

§8.2 中阿丁环的根基是用幂零元、幂零左理想建立的. 1942 年皮里斯(S. Perlis)把幂零元的概念推广，在一般环中引进左拟正则元[11]，1945 年贾柯勃逊用左拟正则元、拟正则左理想把前面的根基概念推广，创造了一般环的根基，建立了一般环的构造理论[3].

假定 a 是有单位元 1 的环中一元，如果 $1+a$ 有左逆，我们把这左逆写成 $1+a'$，那么 $(1+a')(1+a)=1$，因此

$$a + a' + a'a = 0. \tag{1}$$

反过来，假如 a 是环中一元，如果有 a' 满足(1)，那么 $1+a'$ 是 $1+a$ 的左逆元. 在一般环 R 中我们根据(1)引进一个新的结合法，对于

R 中两元 a, a'，我们规定*

$$a \circ a' = a + a' + a'a,$$

这结合法 $\circ$ 叫做 R 的**拟乘法**. 显然，拟乘法满足结合律，并且 R 的零元 0 是它的单位元，即

$$(a \circ b) \circ c = a \circ (b \circ c), a \circ 0 = 0 \circ a = a.$$

当 $a \circ a' = 0$ 时我们叫 a' 是 a 的**右拟逆元**，a 是 a' 的**左拟逆元**，这时，我们又说 a 是 R 的**左拟正则元**，a' 是 R 的**右拟正则元**. R 中元 a，如果是左拟正则元同时又是右拟正则元，那么 a 就叫做 R 的**拟正则元**. 我们容易证明，R 中所有拟正则元对 $\circ$ 成为群 G'，叫做 R 的**圆群**，当 R 有单位元 1 时，这 G' 与 R 中所有可逆元对乘法组成的群 G 同构，$a \to 1 - a$ 就是 G' 射到 G 上的同构映射.

假如 a 是 R 的拟正则元，那么 a 的左拟逆元也是 a 的右拟逆元，因此是 a 的**拟逆元**. 这是因为 $\circ$ 适合结合律：由

$$a \circ a' = 0, a'' \circ a = 0,$$

我们就有

$$a'' = a'' \circ 0 = a'' \circ (a \circ a') = (a'' \circ a) \circ a' = 0 \circ a' = a'.$$

所以 $a \circ a' = a' \circ a = 0$. 即 $a'a = aa'$，因此一个拟正则元的拟逆元是唯一的.

显然，环 R 的零元是 R 的拟正则元. R 的幂零元也是 R 的拟正则元，这是因为，假如 $a^n = 0$，命

$$a' = -a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1},$$

我们容易验证 $a \circ a' = a' \circ a = (-1)^{n-1}a^n = 0$. 但拟正则元一般不是幂零元. 譬如，在由所有有理数 n/m，这里 m 是奇数，n 是任意整数，形成的环中，不含非零的幂零元，但任意形如 $2n/m$ 的元都是拟正则元，这是因为 $\frac{2n}{m} + \frac{-2n}{2n+m} + \frac{2n(-2n)}{m(2n+m)} = 0$.

---

* 有的书中规定 $a \circ a' = a + a' + aa'$，用这个式子，后面的结论都完全成立，只是个别式子不完全一样.

假如环 R 有单位元 1，那么 -1 不是拟正则元，这是因为如果 -1 是拟正则元，那么 $-1+a'+a'(-1)=0$，因此 $-1=0$，这显然是矛盾. 再假如 a 是幂等元，那么 $-a$ 不是左拟正则元，这是因为由 $-a+a'-a'a=0$，得 $-a^2+a'a-a'a^2=0$，即 $-a+a'a-a'a=-a=0$，此不可. 又在体中除 -1 外其他元都是左拟正则元，反过来也成立，即在一环中除一元外其他元都是左拟正则元时，那么这环是体[12].

当环 R 有单位元 1 时，元 r 是 r' 的左拟逆元的必要充分条件是：$1+r'$ 是 $1+r$ 的右逆元，因此在整数环 Z 中只有 0 及 -2 是左拟正则元.

定理 1 环 R 中元 r 是左拟正则元的必要充分条件是：

$$L=\{x+xr \mid x\in R\}=R.$$

证明 因为所有形如 $x+xr, x\in R$ 的元成为 R 的左理想 L. 假如 r 是左拟正则元，那么 $-r=r'+r'r\in L$，因此 $r\in L$，于是 $x\in L$. 所以 $L=R$. 反过来，假如 $L=R$，那么 $-r=r'+r'r$，即 $r+r'+r'r=0$，所以 r 是左拟正则元，于是定理成立.

下面的定义与幂零左理想类似.

定义 1 环 R 的左(右)理想，其中任意元都是 R 的左(右)拟正则元时，叫做 R 的**拟正则左(右)理想**. R 的理想，其中任意元都是 R 的拟正则元时，叫做 R 的**拟正则理想**.

一般，一个左拟正则元不一定又是右拟正则元，假如 L 是环 R 的拟正则左理想，那么其中任意元又是 R 的右拟正则元，因此是 R 的拟正则元. 这是因为，假如 $a\in L$，由 $a\circ a'=0$，得知 a' 是 R 的右拟正则元，但 $a'=-a-a'a\in L$，所以 a' 又是 R 的左拟正则元，因此我们有 $a\circ a'=a'\circ a=0$，即 a 是 R 的拟正则元.

同样，在环 R 的拟正则右理想中任意元也都是 R 的拟正则元. 于是，拟正则左或右理想中元都是拟正则元，拟正则左或右理想如果又是理想，那么它就是拟正则理想.

因为幂零元是拟正则元，所以在一般环中幂零元左理想是拟

正则左理想. 在阿丁环中,反过来也成立,即

定理 2 假定 L 是环 R 的拟正则左理想,如果 R 是阿丁环,那么 L 是幂零左理想.

证明 假定 $L\supset L^2\supset L^3\supset\cdots$,根据极小条件,则有某正整数 k,使 $L^k=L^{k+1}$. 命 $P=L^k$,下面我们用反证法来证明 $P=0$.

假如 $P\neq 0$,我们命 N 是 R 中满足下面条件的极小左理想

$$PN\neq 0.$$

显然 N 是存在的,因为 P 自身就满足这条件. 于是 N 中有元 a 使 $Pa\neq 0$. 因为 $P^2=P$,所以 $P(Pa)=P^2a=Pa\neq 0$,但 $Pa\subseteq N$,而 N 是极小左理想,所以 $Pa=N$. 于是 P 中有元 x 使 $xa=a$,因为 $x\in P$,所以 $-x$ 是 R 的左拟正则元,于是 $-x+x'-x'x=0$,因此

$$-xa+x'a-x'xa=0,$$

即 $a=0$,这与 $Pa\neq 0$ 的假设矛盾. 所以 $P=0$,即 $L^k=0$,这就是说,L 是幂零左理想. 于是定理成立.

现在我们用拟正则左理想代替 § 8.2 中幂零左理想来建立一般环的根基.

下面是与 § 8.2 中类似的定理.

定理 3 假定 L_1,L_2 是环 R 的拟正则左理想,那么它们的和 (L_1,L_2) 也是 R 的拟正则左理想.

证明 假定 $a\in L_1,b\in L_2$,那么我们有

$$a+a'+a'a=0,$$

又因为 $b+a'b\in L_2$,所以我们又有

$$b+a'b+c+c(b+a'b)=0,$$

于是

$$\begin{aligned}&a+b+(a'+c+ca')+(a'+c+ca')(a+b)\\&=(a+a'+a'a)+\{b+a'b+c+c(b+a'b)\}\\&\quad+c(a+a'+a'a)=0,\end{aligned}$$

所以 $a+b$ 是 R 的左拟正则元,因此 (L_1,L_2) 是 R 的拟正则左理想,于是定理成立.

定理 4 环 R 中所有拟正则左理想的和是 R 的拟正则理想，叫做 R 的**贾柯勃逊根基**或简称 R 的**根基**，用 $J(R)$ 或 J 表示.

证明 因为这里和指的是离散的，所以 J 中任意元是 R 中某有穷个拟正则左理想中元的和，由上定理，它是 R 的左拟正则元，所以 J 是 R 的拟正则左理想.

下面我们来证明 J 是 R 的理想. 假定 a 是 J 中任意元，r 是 R 中任意元，如果我们能够证明 $ar\in J$，那么 J 又是 R 的右理想，因此 J 就是 R 的理想了.

假定 L 是由 ar 生成的 R 的左理想，即 L 中任意元可以写成

$$sar+nar=(sa+na)r=tr, t=sa+na,$$

因为 $a\in J$，所以 $t\in J$，因此 $rt\in J$，于是我们有

$$rt+b+brt=0,$$

因此

$$\begin{aligned} &tr+(-tr-tbr)+(-tr-tbr)tr \\ &=-t(b+rt+brt)r=0 \end{aligned}$$

所以 tr 是 R 的左拟正则元. 即 L 中任意元是 R 的左拟正则元，因此 L 是 R 的拟正则左理想，所以 $L\subseteq J$，于是 $ar\in J$. 定理成立.

上面根基概念是根据拟正则左理想建立的. 假如我们把左理想换成右理想，引用拟正则右理想，我们同样可以建立根基. 如果这时得到的是 J'，那么 $J'=J$. 这是因为，J' 是 R 的理想，并且其中任意元是 R 的拟正则元，所以 J' 是 R 的拟正则理想，因此 $J'\subseteq J$. 同样有 $J\subseteq J'$，所以 $J'=J$.

于是 J 既包含 R 的所有拟正则左理想，也包含 R 的所有拟正则右理想. 又因为 R 的幂零元左理想是 R 的拟正则左理想，R 的幂零元右理想是 R 的拟正则右理想，所以 J 又包含 R 的所有幂零元左理想，及所有幂零元右理想. 当 R 是在交换环时，因为任意幂零元生成的理想是幂零元理想，因此交换环 R 的根基 J 包含 R 中所有幂零元，但它可能还包含其他非幂零的拟正则元.

当 R 是阿丁环时由定理 2 得知它的根基 J 中任意元都是幂

零元.

根基中元如果都是幂零元就叫做**幂零元根基**. 阿丁环 R 的根基 N 或它的贾柯勃逊根基 J 都是幂零元根基显然两者是一致的. 一般环的贾柯勃逊根基不是幂零元根基.

定义 2　环 R 如果它的根基 $J=R$, 那么 R 叫做**根基环**, 如果 $J=0$, 那么 R 叫做**半单纯环**, 或简称**半单环**.

有时 § 8.2 中半单环又叫做**幂零半单环**, 这里的半单环又叫做**贾柯勃逊半单环**.

显然, 幂零元环是根基环. 有单位元的环不是根基环, 因为 -1 不是拟正则元. 含有幂等元的环也不是根基环, 因为幂等元不在环的根基中, 再整数环 Z 是半单环, 这是因为 Z 中只有 $0, -2$ 是左拟正则元, 而由 -2 生成的理想是偶数环, 它不是 Z 的拟正则左理想, 由这也说明环的拟正则元不一定都在它的根基中.

根基环对拟乘法形成群, 即根基环是圆群[13].

定理 5　假定 J 是环 R 的根基, 那么 $\overline{R}=R-J$ 是半单环.

证明　假定 $\overline{L}=L-J$ 是 $\overline{R}$ 中任意拟正则左理想, $\bar{a}$ 是 $\overline{L}$ 中任意元, 那么在 $\overline{R}$ 中有元 $\bar{a}'$ 使 $\bar{a}+\bar{a}'+\bar{a}'\bar{a}=\bar{0}$, 所以

$$a+a'+a'a\in J,$$

于是 R 中有元 u, 使

$$a+a'+a'a+u+u(a+a'+a'a)=0,$$

即

$$a+(a'+u+ua')+(a'+u+ua')a=0.$$

因此 a 是 R 的左拟正则元, 所以 L 是 R 的拟正则左理想, 因此 $L\subseteq J$. 于是 $\overline{L}=\bar{0}$, 这就是说, $\overline{R}$ 中任意拟正则左理想是零理想, 所以 $\overline{R}$ 的根基是零, 因此 $\overline{R}$ 是半单环. 于是定理成立.

定理 6　假定 R 是环, 那么全矩阵环 R_n 的根基 $J(R_n)$ 是 R 的根基 $J(R)$ 上的全矩阵环 $(J(R))_n$, 即 $J(R_n)=(J(R))_n$.

证明　我们先证明 $J(R_n)\subseteq(J(R))_n$.

假定 L_{ij} 是 $J(R_n)$ 中矩阵的第 i 行第 j 列上元的集合, 显然 L_{ij}

是 R 的理想. 命 rE_{ij} 是第 i 行第 j 列上元是 R 中元 r、其余元都是零的 n 阶矩阵，那么

$$RE_{1i}J(R_n)E_{j1}R\subset J(R_n),$$

因此 $RL_{ij}RE_{11}\subset J(R_n)$，即

$$\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}\in J(R_n),a\in RL_{ij}R.$$

于是它是左拟正则元. 因此我们有

$$\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}+\begin{pmatrix} a_{11}' & \cdots & a_{1n}' \\ \cdots & \cdots & \cdots \\ a_{n1}' & \cdots & a_{nn}' \end{pmatrix}+\begin{pmatrix} a_{11}' & \cdots & a_{1n}' \\ \cdots & \cdots & \cdots \\ a_{n1}' & \cdots & a_{nn}' \end{pmatrix}\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}=\begin{pmatrix} a & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix},$$

所以 $a+a'_{11}+a'_{11}a=0$，这就是说，$RL_{ij}R$ 中任意元是 R 的左拟正则元，因此 $RL_{ij}R$ 是 R 的拟正则理想. 于是 $RL_{ij}R\subset J(R)$，所以 $RL_{ij}RL_{ij}\subset J(R)$，即 $(\overline{R}\overline{L}_{ij})^2=\overline{0}$，但 $\overline{R}=R-J$ 的根基是零，因此 $\overline{R}\overline{L}_{ij}=\overline{0}$，又因为 $\overline{L}_{ij}^2\subseteq\overline{R}\overline{L}_{ij}=\overline{0}$，所以 $\overline{L}_{ij}=\overline{0}$. 即 $L_{ij}\subset J(R)$，这就是说，假如 $(a_{ij})\in J(R_n)$，那么 $a_{ij}\in J(R)$，所以 $J(R_n)\subseteq(J(R))_n$.

我们再来证明 $(J(R))_n\subseteq J(R_n)$. 我们来考虑所有形如

$$A_1=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix},a_{i1}\in J(R),$$

的 n 阶矩阵集合 M_1，显然 M_1 是 R_n 的左理想. 假定

$$A'=\begin{pmatrix} a_{11}' & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix},a_{11}+a_{11}'+a_{11}'a_{11}=0,$$

那么

$$A_1\circ A'=\begin{pmatrix} 0 & \cdots & 0 \\ a_{21} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & 0 \end{pmatrix},$$

因此$(A_1\circ A')^2=0$，即$A_1\circ A'$是幂零元，所以它也是左拟正则元．于是有$(A_1\circ A')\circ B=0, B\in R_n$，即$A_1\circ(A'\circ B)=0$．这就是说，$A_1$是$R_n$的左拟正则元，所以$M_1$是$R_n$的拟正则左理想．同样，所有第$i$列是$J(R)$中元，其余元都是零的$n$阶矩阵$A_i$的集合$M_i$成为$R_n$的拟正则左理想．因此$M_1+\cdots+M_n$也是$R_n$的拟正则左理想．所以它在$J(R_n)$中．再因为$(J(R))_n$中任意元可以写成如$A_1$，$\cdots$，$A_n$这样的$n$个矩阵的和，因此它在$M_1+\cdots+M_n$中；这就是说，$(J(R))_n$中任意元都在$J(R_n)$中，即$(J(R))_n\subseteq J(R_n)$．因此定理成立．

与§2定理8类似，环的根基与它的理想的根基的关系，我们有下面定理．

定理 7 假定N是环R的理想，那么

$$J(N)=N\cap J(R).$$

证明 假定$a\in N\cap J(R)$，因为$a\in J(R)$，所以R中有元a'使$a+a'+a'a=0$．又因为$a\in N$，所以$a'a\in N$，因此$a'=-a-a'a\in N$，即a是N的左拟正则元，于是$N\cap J(R)$是N的拟正则左理想．所以它在$J(N)$中，即$N\cap J(R)\subseteq J(N)$．

下面证明$J(N)\subseteq J(R)$．设$a\in J(N)$，那么

$$NRaRN\subseteq NaN\subseteq J(N),$$

因此$RaR\subseteq J(N)$(根据后面的习题5)．即RaR是R中拟正则理想，所以$RaR\subseteq J(R)$．因此我们又有$a\in J(R)$．于是$J(N)\subseteq J(R)$．

定理证毕．

于是，半单环的理想仍然是半单环．这与§8.3定理3是一致的．一个环的根基自身是根基环，即$J(J(R))=J(R)$．但根基环的子环不一定是根基环[14]．

在后面讨论时，常常需要下面这样的左理想．

定义 3 假如L是环R的左理想，如果R中有元e，对于R中任意元x，有$x-xe\in L$，即$x\equiv xe(L)$，那么L叫做R的正则左理

想，e 叫做 R 对于 L 的**右单位元**.

显然，当环 R 有单位元时，它的任意左理想是正则左理想. 假如环 R 的左理想包含 R 的某正则左理想，那么它自身也是正则左理想. 也就是说，正则左理想的扩张左理想仍然是正则左理想.

譬如在偶数环 R 中，理想(6)是正则左理想，它的 $e=4$，即 4 是 R 对于(6)的右单位元，理想(4)不是正则理想.

定理 8 假定环 R 中元 a 不是左拟正则元，那么 R 有不包含 a 的极大正则左理想.

证明 因为 a 不是左拟正则元，所以 R 的左理想

$$L=\{x+xa \mid x\in R\}$$

不包含 a，这是因为，如果 $a\in L$，那么 $L=R$，这与定理 1 矛盾. 于是 R 中所有包含 L 而不包含 a 的左理想，根据集合的包含，由冲恩引理，我们有包含 L 而不包含 a 的极大左理想. 这左理想，显然也是 R 的极大理想，因为如果另有包含它的左理想，那么它就要包含 a，因此它就是 R 了. 因为 L 是正则左理想，所以这包含 L 的极大左理想也是正则的. 因此定理得证.

于是得知，假如 R 不是根基环，那么 R 有极大正则左理想. 下面主要是介绍根基的性质.

定理 9 环 R 的根基 J 是 R 的所有极大正则左理想的交集：

$$J=\bigcap M_i,$$

M_i 是 R 的极大正则左理想.

证明 假定 $a\in\bigcap M_i$，即 a 在 R 的任意极大正则左理想中. 如果 a 不是左拟正则元，由上定理，R 就有不包含 a 的极大正则左理想. 这与假设不合，所以 a 是左拟正则元. 于是 $\bigcap M_i$ 是 R 的拟正则左理想. 因此 $\bigcap M_i\subseteq J$.

再假定 $a\overline{\in}\bigcap M_i$，那么 R 中有某极大正则左理想 M 不包含 a，因为 M 是极大左理想，所以由 M 及 a 生成的左理想就是 R 自身，即

$$R=\{m+(ra+na)\}.$$

这里 $m\in M,r\in R,n$ 是整数或零. 如果 e 是 R 对于 M 的右单位元，那么 $-e=m_1+(ra+na)$，即 $-(e+m_1)=ra+na$. 因为 $e+m_1$ 也是 R 对于 M 的右单位元，由定理 1，$e+m_1$ 的负元不是左拟正则元，即 $ra+na$ 不是左拟正则元，这就是说，由 a 生成的左理想不是拟正则左理想，所以 $a\overline{\in}J$. 因此 $J\subseteq\bigcap M_i$. 于是 $J=\bigcap M_i$. 定理证毕.

假如 R 有单位元，那么它的左理想都是正则左理想，因此 R 的根基 J 是 R 的所有极大左理想的交集.

我们知道，幂零半单环(定义 2)的构造归结为单环的构造，与这类似，贾柯勃逊半单环的构造归结为本原环的构造. 本原环是单纯环的推广，是一类非常重要的环. 下面介绍本原环，先介绍一个基本性质.

假定 M 是 R 的左理想，显然

$$(M:R)=\{r\mid r\in R,rR\subseteq M\}$$

是 R 的理想. 如果 N 是 R 的理想，并且 $N\subseteq M$，那么 $NR\subseteq M$，因此 $N\subseteq(M:R)$，这就是说，R 的理想如果包含在 M 中，它也包含在$(M:R)$中. 假如$(M:R)\subseteq M$，那么$(M:R)$就是 R 中包含在 M 的最大理想. 假如$(M:R)=0$，那么 M 不包含 R 中非零的理想.

定理 10 假定 M 是环 R 的正则左理想(不一定极大)，那么$(M:R)\subseteq M$，因此$(M:R)$是 R 中包含在 M 的最大理想.

证明 假定 $a\in(M:R)$，那么 $aR\subseteq M$，如果 e 是 R 对于 M 的右单位元，那么 $a-ae\in M$，因为 $ae\in M$，所以 $a\in M$. 于是$(M:R)\subseteq M$. 因此定理成立.

定义 4 假如 M 是 R 的极大左理想，如果$(M:R)=0$，那么 R 叫做(左)**本原环**. 假如 N 是 R 的理想，如果 $\overline{R}=R-N$ 是本原环，那么 N 叫做 R 的(左)**本原理想**.

显然，零环不是本原环，本原环的零理想是本原理想，再体 K 是本原环，因为它的极大左理想是零理想，并且$((0):K)=0$. 整数环 Z 不是本原环，因为(p)是它的极大理想，但$((p):Z)=$

(p). 再因为 $Z-(p)$ 是体，所以它是本原环，因此 (p) 是 Z 的本原理想. 1961 年柏生尔(E. C. Posner，1933～，Kaplansky 的学生)曾证明环 R 是本原环的必要充分条件是全矩阵环 R_n 是本原环[15].

一个左本原环是否又是右本原环，这是环论中长期没有得到解决的一个问题，1964 年柏尔门(G. M. Bergman)给出了一个左本原环但不是右本原环的例[16]解答了这问题.

定理 11 假定 M 是 R 的极大正则左理想，那么 $(M:R)$ 是 R 的本原理想.

证明 由定理 10，我们得知 $(M:R)\subseteq M$，显然 M 在 $\overline{R}=R-(M:R)$ 的象 $\overline{M}$ 是 $\overline{R}$ 的左理想，因为 M 是 R 的极大左理想，所以 $\overline{M}$ 是 $\overline{R}$ 的极大左理想. 再 $(\overline{M}:\overline{R})=\overline{0}$，这是因为，假如 $\overline{a}\overline{R}\subseteq\overline{M}$，那么 $aR\subseteq M$，因此 $a\in(M:R)$，所以 $\overline{a}=\overline{0}$，于是 $\overline{R}$ 是本原环，因此 $(M:R)$ 是本原理想.

定理证毕.

于是，假如 R 不是根基环，那么它有极大正则理想，因此 R 有本原理想.

定理 12 环 R 的根基 $J(\neq R)$ 是 R 的所有本原理想 N_i 的交集，即

$$J=\bigcap N_i.$$

证明 因为 J 是 R 的所有极大正则左理想的交集. 又因为 R 的任意极大正则 左理想 M 包含本原理想 $(M:R)$，所以 J 包含 R 的某些本原理想的交集，因此 J 更包含 R 的所有本原理想的交集. 下面我们来证明，J 包含在 R 的任意本原理想中，因此 J 就是 R 的所有本原理想的交集，于是定理就告成立.

假定 N 是 R 的任意本原理想，那么 $\overline{R}=R-N$ 是本原环. 因此 $\overline{R}$ 有极大左理想 $\overline{M}$，使 $(\overline{M}:\overline{R})=\overline{0}$. 于是 $(M:R)\subseteq N$. 因为 $N\subseteq M$，所以 $(M:R)\subseteq M$. 因此 $(M:R)$ 就是 R 中包含在 M 的最大理想. 假如我们能够证明 $J\subseteq M$，那么 $J\subseteq(M:R)$，因此 $J\subseteq N$，定理就得证.

我们先证明

$$L=\{r\mid r\in R, Rr\subseteq M\}=M.$$

这是因为，L 是 R 的左理想，并且包含 M，因为 M 是极大，所以 L 是 M 或者是 R. 如果 $L=R$，那么 $RR\subseteq M$，于是 $(M:R)=R$，但 $(M:R)\subseteq M$，所以 $M=R$，这与假设不合. 因此 $L=M$.

再用反证法. 假设 $J\not\subseteq M$，并且 $a\in J, a\overline{\in} M$. 如果 $aR\subseteq M$，那么 $a\in(M:R)\subseteq M$，这不可. 因此 $aR\not\subseteq M$. 命 $b\in R, ab\overline{\in} M$，因为 $L=M$，所以 $Rab\overline{\in} M$. 但 M 是极大，因此 $(M, Rab)=R$. 于是存在 $m\in M, r\in R$，使 $m+rab=-b$，即 $b+rab=-m\in M$. 再因为 $a\in J$. 所以 ra 是左拟正则元，因此有元 c 使 $ra+c+cra=0$. 于是

$$b=b+(ra+c+cra)b=(b+rab)+c(b+rab)\in M.$$

这与 $ab\overline{\in} M$ 的假设矛盾. 因此 $J\subseteq M$.

于是定理成立.

因为本原环的零子环是本原理想，所以本原环的根基是零，这就是说，本原环是半单环. 除零环外，本原环不是根基环.

定理 13 单环是根基环或是本原环.

证明 假定 R 是单环，$R^2=R$. 如果 R 不是根基环，那么 R 有极大左理想 M. 于是 $(M:R)$ 是 R 的理想. 所以

$$(M:R)=0 \text{ 或 } (M:R)=R.$$

如果 $(M:R)=R$，那么 $RR=R^2\subseteq M$，即 $R^2=R\subseteq M$，这与 $M\subset R$ 的假设矛盾. 因此 $(M:R)=0$. 所以 R 是本原环. 于是定理成立.

子是单环有单位元时是本原环，但有单位元的本原环不一定是单环.

定理 14 假定单环 R 有左理想或右理想 L，那么 R 是本原环[18].

证明 用反证法. 假定 L 是 R 的左理想，如果 R 不是本原环，那么 $R^2=0$. 因此 $LR\subseteq R^2=0$，即 L 是 R 的理想. 此不可，所以 R 是本原环. 证毕.

单根基环是否存在是环论中一个悬而未决的问题，1961 年沙

士亚大(E. Sasiada)预言这种环是存在的,1967 年他给出一个具体的例来说明[17],但他给出的不是幂零元环. 因此,现在存在的问题是有没有单纯幂零元环.

习 题 8.5

1. 假如 a 是拟正则左理想 L 中元,那么满足(1)的 a' 是唯一的,并且 $aa'=a'a$.

2. 假定 a 是 R 中元,如果 $-a^2$ 是左拟正则元,那么 a 也是 R 的左拟正则元.

3. 假定 $a\in R$,a^n 是左拟正则元,n 是奇数,那么 a 也是左拟正则元.

4. 假如 a,b 是环 R 中元,如果 ab 是左拟正则元,那么 ba 也是左拟正则元.

5. 假定 $x\in R$,如果 Rx,xR 或 RxR 有一在 R 的根基 J 中,那么 $x\in J$.

6. 假如 a 是环 R 的根基 J 中元,那么 R 中满足 $x=ax$ 的元 x 只有零元,即 $x=0$.

7. 假如 a 是环 R 的根基 J 中元,如果 $a^n=a^m$,$n>m$,那么 $a^m=0$.

8. 假如 1 是环 R 的单位元,$a\in J$,那么 $1+a$ 有逆元.

9. 假定 σ 是环 R 到环 S 的同态,那么 $\sigma(J(R))\subseteq J(S)$.

10. 任意正则左理想能够嵌入极大正则左理想.

11. 假定 R 是根基环,那么它没有正则左理想.

12. 试证正则环是半单环.

13. 假定 R 是所有这样的有理数 $\frac{n}{m}$ 构成的环,其中 m 是奇数,n 是任意整数,试证 R 的根基是(2),它不包含非零的幂零元.

14. 假如 R 是有单位元的环,如果其中所有不是可逆元的元形成理想 N,那么 N 是 R 的根基.

15. 试证 $J(eRe)=eJ(R)e$,这里 e 是环 R 的幂等元.

16. 假定 N 是环 R 的本原理想,那么 R 中存在极大左理想 M,使得 $N=(M:R)$.

§8.6 次 直 和

我们知道根基是零的环叫做半单环. 这节我们讨论半单环的

构造，它是 用次直和表达的，是 § 8.3 中幂零半单环构造的推广.

我们先介绍次直和这个新概念. 我们知道，在 § 6.4 中我们讨论了环的直和，但是很多时候，环不能写成为若干个环的直和，却能够写成为若干个环的直和的子环，这样把直和推广就创造了次直和这个概念[19].

假定有两个环 $R_1=Z-(2)$ 及 $R_2=Z-(4)$，即

$$R_1=\{0_1,1_1\},R_2=\{0_2,1_2,2_2,3_3\},$$

那么
$$S_1=\{(0_1,0_2),(1_1,1_2),(0_1,2_2),(1_1,3_2)\},$$
$$S_2=\{(0_1,0_2),(0_1,2_2),(1_1,0_2),(1_1,2_2)\}$$

都是 R_1,R_2 的直和 R_1+R_2 的子环. 但它们有区别，在 S_1 中，R_1,R_2 中元都完全出现，但在 S_2 中，R_1 中元都出现而 R_2 中元不完全出现，这时显然

$(0_1,0_2)\to 0_1,(1_1,1_2)\to 1_1,(0_1,2_2)\to 0_1,(1_1,3_2)\to 1_1$ 是 S_1 到 R_1 上的同态，

$$(0_1,0_2)\to 0_2,(1_1,1_2)\to 1_2,(0_1,2_2)\to 2_2,(1_1,3_2)\to 3_2$$

是 S_1 到 R_2 上的同态. 也就是说，这时 $S_1\sim R_i, i=1,2$，但 S_2 就没有这个性质，我们把 S_1 叫做 R_1,R_2 的次直和. 一般我们有

定义 1 假定 $\{R_i|i\in I\}$ 是一组环 R_i 的集合，R 是 $\{R_i\}$ 的完全直和 ΣR_i 中由

$$r=(r_i|r_i\in R_i)$$

组成的子环，如果

$$r\to r_i, i\in I$$

是 R 到 R_i 上的同态，即 $R\sim R_i$，那么 R 叫做 $\{R_i\}$ 的**次直和**.

显然 $\{R_i\}$ 的完全直和是 $\{R_i\}$ 的次直和. 要注意的是，$\{R_i\}$ 的完全直和是由 $\{R_i\}$ 唯一确定的，但 $\{R_i\}$ 的次直和不由 $\{R_i\}$ 唯一决定，它有各种不同的次直和.

再我们容易得知，$\{R_i\}$ 的完全直和的子环是 $\{R_i\}$ 的次直和，这里 R'_i 是 R_i 的子环. $\{R_i\}$ 的次直和是 $\{R_i^*\}$ 的完全直和的子环，这里 R_i^* 是 R_i 的扩张环.

我们先给出环是次直和的必要充分条件.

定理 1 环 R 是环 $\{R_i | i\in I\}$ 的次直和的必要充分条件是 R 中有理想 $\{N_i | i\in I\}$，并且

$$\bigcap N_i=0, R_i\simeq R-N_i.$$

证明 假定 R 是 $\{R_i\}$ 的次直和，由定义我们有 $R\sim R_i$，所以 $R_i\simeq R-N_i$，这里 N_i 是同态核. 因此 N_i 是 R 的理想. 再假如 $\{r_i | r_i\in R_i\}\in\bigcap N_i$，那么 r_i 是 R_i 的零元，即 $r_i=0$，因此 $\bigcap N_i=0$. 所以条件的必要性成立.

反过来，假如 N_i 是 R 的理想，并且 $\bigcap N_i=0$. 我们命 $R_i=R-N_i$，σ_i 是 R 到 R_i 上的同态，N_i 是它的同态核，于是对于 R 中任意元 r，我们有 $\sigma_i(r)=r_i\in R_i$. 显然在 $\{R_i\}$ 的完全直和中由所有这样的

$$\{r_i\}, \sigma_i(r)=r_i\in R_i$$

组成的环 R' 是 $\{R_i\}$ 的次直和. 下面我们来证明 R 与 R' 同构.

我们命 R 中元 r 与 $\{r_i\}$ 对应，即

$$r\to\{\sigma_i(r)\}$$

显然它是 R 到 R' 上的映射. 又因为

$$\sigma_i(r+s)=\sigma_i(r)+\sigma_i(s), \sigma_i(rs)=\sigma_i(r)\sigma_i(s),$$

所以
$$r+s\to\{\sigma_i(r+s)\}=\{\sigma_i(r)\}+\{\sigma_i(s)\}$$
$$r\cdot s\to\{\sigma_i(rs)\}=\{\sigma_i(r)\cdot\sigma_i(s)\}$$

于是 R 与 R' 同态，即 $R\sim R'$，再因为 $\sigma_i(r)=0$ 时，$r\in N_i$，但 $\bigcap N_i=0$，所以 $r=0$，因此 $R\simeq R'$. 这就是说，R 与 $\{R_i\}$ 的次直和同构，所以条件的充分性成立.

于是定理得证.

下面是贾柯勃逊关于半单环的主要构造定理.

定理 2 半单环是本原环的次直和.

证明 根据§8.5 定理12，R 的所有本原理想 N_i 的交集 $\bigcap N_i=0$，于是由上定理，R 是 $\{R-N_i\}$ 的次直和. 又因为 N_i 是 R 的本原理想，所以 $R-N_i$ 是本原环. 因此定理成立.

于是我们又得到

定理3 假定环 R 的根基是 J，那么 $R-J$ 是本原环的次直和.

下面是定理2的逆.

定理4 假定 R 是本原环 $\{R_i\}$ 的次直和，那么 R 是半单环.

证明 由定理1我们有 $R_i\simeq R-N_i$，$\bigcap N_i=0$，因为 R_i 是本原环，所以 N_i 是本原理想，于是由§8.5定理12得知 $J(R)=\bigcap N_i=0$，所以 R 是半单环，定理成立.

最后，我们介绍交换环的几个重要性质.

我们知道域是本原环，它的逆也成立.

定理5 交换本原环是域.

证明 假定 R 是交换本原环，M 是它的极大左理想，$(M:R)=0$. 因为 R 是交换的，所以 $M\subseteq(M:R)$，因此 $M=0$. 这就是说，零理想是 R 的极大理想，即 R 除零理想外，没有其他理想. 再因为 R 的根基是零，所以它不是幂零元环. 由§3.6定理1，R 是体. 因此定理成立.

于是，我们得知交换环是本原环的必要充分条件是它是域.

由定理2及上定理我们又得到

定理6 元数大于1的交换半单环是域的次直和.

下面是比这广泛的定理，由§3.8的定理2我们立即推得

定理7 假如交换环不含非零的幂零元，那么它是整环的次直和.

证明 假定交换环 R 不含非零的幂零元，由§3.8的定理2得知 R 的所有质理想 $\{P_i\}$ 的交集 $\bigcap P_i=0$，设 $R_i\simeq R-P_i$，于是由定理1，环 R 是 $\{R_i\}$ 的次直和. 因为 P_i 是质理想，所以 R_i 是整环. 因此 R 是整环 $\{R_i\}$ 的次直和. 于是定理成立.

我们还知道，一个环是域 $Z-(2)$ 的次直和的必要充分条件是：它是布尔环. 一个环，如果它的特征数是质数 p，并且对任意元 a 有 $a^p=a$，那么这个环叫 p-环. p-环是有单位元的交换环[20]. 一

个环是域 $Z-(p)$ 的次直和的必要充分条件是：它是 p-环. 这些证明我们都从略[21].

习 题 8.6

1. 在交换环中，本原理想是质理想，但质理想不一定是本原理想，这是为什么？

§8.7 本原环、稠密环

我们知道，假如 M 是环 R 的极大左理想，如果 $(M:R)=0$，那么 R 就是本原环. 前面我们已经介绍了本原环，这节我们将进一步讨论本原环的构造，与 §8.4 所述的类似，主要就是证明下面著名的贾柯勒逊密度定理.

定理 1 假定 R 是本原环，M 是它的极大左理想，$(M:R)=0$，E 是加群 $\overline{R}=R-M$ 的自同态环，

$$R'=\{a'\mid a'\in E, a'\overline{r}=\overline{ar}, a\in R, \overline{r}\in\overline{R}\}$$

是 E 中与 R 同构的子环，

$$F=\{\alpha\mid \alpha\in E, \alpha r'=r'\alpha, r'\in R'\}$$

是体，那么 R 是 F 的向量空间 $\overline{R}$ 的线性变换的稠密环.

下面我们来分段证明.

首先我们与 §3.3 定理 2 类似来证明 R' 与 R 同构. 因为 M 是 R 的左理想，所以 $\overline{R}=R-M$ 是加群. 又因为 a' 是 $\overline{R}$ 的自同态，由 $a'+b'=(a+b)'$，$a'b'=(ab)'$，显然 $a\to a'$ 是 R 到 R' 上的同态. 再因为 $a'=0$ 时 $\overline{ar}=\overline{0}$，得 $ar\in M$，所以 $a\in(M:R)=0$. 因此上述同态是同构. 于是 $R\simeq R'$.

我们再来证明 F 是体.

定理 2 假定 F 是 E 中所有与 R' 中任意元能够交换的元集，那么 F 是体.

证明 F 显然是环，并且有单位元，因为 E 有单位元.

假定 α 是 F 中非零元，那么 $\{\alpha\bar{r}\}$ 是 $\bar{R}=R-M$ 对于 α 的象集，我们先来证明 $\{\alpha\bar{r}\}=\bar{R}$，因此 α 是 $\bar{R}$ 到 $\bar{R}$ 上的自同态.

我们知道 α 是 $\bar{R}$ 的自同态，当 $\alpha\bar{r}=\bar{s}$ 时，我们规定 $\alpha r=s$，这 s 显然不能由 r 唯一决定，但它们相差只不过是 M 中一个元，与我们的讨论无甚关系，因此 $\alpha\bar{r}=\overline{\alpha r}$，今 $\alpha\neq 0$，所以 $\{\alpha\bar{r}\}\neq\bar{0}$. 因此 R 中有元 r 使 $\alpha\bar{r}\neq\bar{0}$. 于是 $\alpha r\,\bar{\in}\, M$，但 M 是极大左理想，所以由 M 及 αr 生成的左理想就是 R. 于是对于 R 中任意元 x，我们就有

$$x=m+a\alpha r+n\alpha r, m\in M, a\in R, n \text{ 是整数或零},$$

因为 $\alpha\in F$，所以 $a'\alpha\bar{r}=\alpha a'\bar{r}$，因此 $\overline{a\alpha r}=\overline{\alpha ar}$，于是 $x=m+\alpha(ar+nr)$，所以 $\bar{x}=\overline{\alpha(ar+nr)}$，这就是说，对于 R 中任意元 x，我们有 $\bar{x}\in\{\alpha\bar{r}\}$，即 $\{\alpha\bar{r}\}=\bar{R}$.

我们再来证明 α 是 $\bar{R}$ 的自同构.

假定 $\alpha\bar{r}=\bar{0}$，那么 $\alpha r\in M$，如果 $r\,\bar{\in}\, M$，因为 M 是极大左理想，所以对于 R 中任意元 x，可以写成 $x=m+ar+nr$，所以

$$\alpha x=\alpha m+\alpha ar+\alpha nr=\alpha m+a\cdot\alpha r+n\alpha r\in M,$$

即 $\alpha\bar{x}=\bar{0}$，这与 $\alpha\neq 0$ 的假设不合. 于是 $r\in M$. 这就是说，$\alpha\bar{r}=\bar{0}$时 $\bar{r}=\bar{0}$，所以 α 是同构.

于是在 E 中 α 有逆 α^{-1}，因为 $\alpha r'=r'\alpha$，所以 $\alpha^{-1}r'=r'\alpha^{-1}$，因此 $\alpha^{-1}\in F$. 于是 F 是体，所以定理成立.

因为 F 中元是 $\bar{R}$ 的自同态，所以 $\bar{R}$ 是 F 的向量空间，于是我们有

定理 3 $\bar{R}=R-M$ 是体 F 的左向量空间，R' 中元是 F 向量空间 $\bar{R}$ 的线性变换.

$\bar{R}$ 一般虽是 F 的无穷维向量空间，但 R' 中元是 F 向量空间 $\bar{R}$ 的线性变换，我们可以同 §8.4 中一样，把 R' 中元用元素是 F 中元的无穷阶矩阵表示. 我们不这样做，因为这样我们就很难再推得其他性质，我们用另一个概念来表达.

下面，我们先介绍稠密环这个重要概念.

定义 假定 V 是体 F 的(左)向量空间，T 是 V 的线性变换集

合，如果对于 V 中任意 n 个线性无关的元 $x_1,\cdots,x_n$ 及任意 n 个元 $y_1,\cdots,y_n$，在 T 中存在着 $x_i\to y_i$ 的线性变换，那么 T 叫做对于 V 是 n 重可迁. 如果对于任意 n，T 对于 V 都是 n 重可迁，那么 T 叫做对于 V 是稠密的. 假如 T 又成环，那么 T 又叫做 V 的线性变换的稠密环，或简称稠密环.

假如 T 对于 V 是 n 重可迁，显然 T 对于 V 是任意 $m(<n)$重可迁.

这里 V 一般是无穷维向量空间而不是有穷维向量空间. 假如 V 是 F 的 n 维空间，由线代数得知，V 的所有线性变换形成的环就是全矩阵环 F_n. 又因为在 V 的线性变换中有把 V 中任意 n 个线性无关的元变为任意 n 个元的线性变换，因此 F_n 是 V 的稠密环，于是(非幂零)阿丁单环是稠密环. 因此魏特邦阿丁第二构造定理是密度定理的特例.

下面我们来证明 R' 是 F 向量空间 $\overline{R}$ 的稠密环.

首先我们来证明 R' 对于 F 向量空间 $\overline{R}$ 是 1 重可迁. 假定 $\overline{0}\neq\overline{x}\in\overline{R}$，那么

$$L=\{rx+m\mid r\in R,m\in M\}$$

是 R 的左理想，因为 M 是极大，所以 $L=R$ 或 $L=M$. 如果 $L=M$，那么 $rx\in M$，因此

$$R=\{m+nx\mid m\in M,n=\text{整数}\},$$

于是 $(M:R)=R$，这与假设矛盾，所以 $L=R$，于是 $R=\{rx+m\}$. 因为 $\overline{R}=R-M$，所以 $\overline{R}=\{\overline{rx}\}=\{r'\overline{x}\}$，即 $R'\overline{x}=\overline{R}$，这就是说，对于 $\overline{R}$ 中任意 $\overline{x}\neq\overline{0}$，$\overline{y}$，在 R' 中有元 r' 使 $r'\overline{x}=\overline{y}$. 因此 R' 对于 $\overline{R}$ 是 1 重可迁.

再假定 $\overline{x}_1,\cdots,\overline{x}_n$ 是 $\overline{R}$ 中 n 个线性无关的元，$\overline{y}_1,\cdots,\overline{y}_n$ 是 $\overline{R}$ 中任意 n 个元，如果在 R' 中能够找到 a_i' 使

$$a_i'\overline{x}_i\neq\overline{0},a_i'\overline{x}_j=\overline{0},i\neq j,$$

因为 R' 已是 1 重可迁，所以在 R' 中有元 b_i'，$i=1,\cdots,n$，使

$$b_i'(a_i'\overline{x}_i)=\overline{y}_i.$$

命 $a'=b_1'a_1'+\cdots+b_n'a_n'$，那么

$$a'\bar{x}_i=(b_1'a_1'+\cdots+b_n'a_n')\bar{x}_i=b_i'a_i'\bar{x}_i=\bar{y}_i,$$

所以，只要下面的定理成立，R' 就是 $\bar{R}$ 的 n 重可迁，因此 R' 是 $\bar{R}$ 的稠密环了.

定理 4 假定 $\bar{W}$ 是 F 向量空间 $\bar{R}=R-M$ 的 n 维子空间，$\bar{x}\in\bar{R}$，$\bar{x}\bar{\in}\bar{W}$，那么 R' 中有元 a' 使 $a'\bar{W}=0$，$a'\bar{x}\neq 0$.

证明 我们用归纳法来证明.

当 $n=0$ 时 $\bar{W}=0$，这时 $R'\bar{W}=0$. 根据前面证得性质，对于 $\bar{x}\neq 0$ 有 $R'\bar{x}=\bar{R}$，这就是说，R' 中有元 a' 使 $a'\bar{x}\neq 0$，显然 $a'\bar{W}=0$，因此 $n=0$ 时定理成立.

假定对维数小于 n 的子空间定理成立，下面我们来证明 $\bar{W}$ 的维数是 n 时定理仍成立.

我们把 $\bar{W}$ 写成 $\bar{W}=\bar{W}_1+F\bar{y}$，这里 $\bar{W}_1$ 是 F 空间 $\bar{R}$ 的 $n-1$ 维子空间. 命 R' 中所有零化 $\bar{W}_1$ 的集合为 S'，即 $S'\bar{W}_1=0$. 根据归纳法假设，$S'\bar{y}\neq 0$，显然 S' 是 R' 的左理想，因此 $S'\bar{y}$ 是 $\bar{R}$ 的左理想，由 $R\sim\bar{R}$. 得知 $S'\bar{y}$ 在 R 的完全象源是 R 中包含 M 的左理想，因此它就是 R 自身，于是 $S'\bar{y}=\bar{R}$. 假如 R' 中零化 $\bar{W}$ 的元也同时都零化 $\bar{x}$，我们命 $a'\bar{y}\to a'\bar{x}$，$a'\in S'$，那么这映射是 $\bar{R}$ 的自同态，这是因为，由 $a_1'\bar{y}\to a_1'\bar{x}$，$a_2'\bar{y}\to a_2'\bar{x}$，如果 $a_1'\bar{y}=a_2'\bar{y}$，那么 $(a_1'-a_2')\bar{y}=0$，但 $a_1'-a_2'\in S'$，所以 $a_1'-a_2'$ 零化 $\bar{W}_1$，同时又零化 $\bar{y}$，因此零化 $\bar{W}$. 根据假设，它也零化 $\bar{x}$，即 $a_1'\bar{x}=a_2'\bar{x}$. 用 α 表示这自同态，于是 $\alpha(a'\bar{y})=a'\bar{x}$. 再由 $\alpha(r'a\bar{y})=r'a'\bar{x}$，得 $\alpha(r'(a'\bar{y}))=r'(\alpha(a'\bar{y}))$，所以 $\alpha r'=r'\alpha$，即 α 与 R' 中任意元能够交换，因此 $\alpha\in F$. 于是 $a'(\bar{x}-\alpha\bar{y})=0$，即 $S'(\bar{x}-\alpha\bar{y})=0$. 根据归纳法假设，$\bar{x}-\alpha\bar{y}\in\bar{W}_1$，所以 $\bar{x}\in\bar{W}_1+\alpha\bar{y}\in\bar{W}$. 这与 $\bar{x}\bar{\in}\bar{W}$ 的假设矛盾，因此 R' 中零化 $\bar{W}$ 的元不同时都零化 $\bar{x}$，所以定理成立.

密度定理至此完全得证. 仿之，我们不难得到下定理——

定理 5 假定 V 是体 F 的向量空间，E 是 V 的自同态环，R 是 E 的子环，即 R 是 V 的线性变换形成的环，如果下面二条件：

1）R 对于 V 是 1 重可迁；

2）V 的自同态环 E 中所有与 R 中任意元能够交换的元形成的环就是 F

成立，那么 R 就是 F 空间 V 的稠密环.

这定理在引用时有时较定理 1 方便.

定理 6 假定 V 是体 F 的向量空间，R 是 V 的线性变换形成的环，如果 R 对于 V 是 2 重可迁，那么 R 是 F 空间 V 的稠密环.

证明 只要我们证明在 V 的自同态环中所有与 R 中任意元能够交换的元 s 是在 F 中，那么 R 就是 V 的稠密环了.

假定 x 是 V 中非零的元，如果 x，sx 线性无关，那么在 R 中有元 r，使 $rx=0$，$rsx\neq 0$，于是 $srx\neq 0$，这与 $rx=0$ 矛盾. 所以 x，sx 线性相关，因此在 F 中有元 α_x 使

$$\alpha_x x=sx.$$

再假设 $y\neq 0$，同样我们有 $\alpha_y y=sy$. 命 $y=ax$，$a\in R$. 于是

$$\alpha_y y=sy=s(ax)=a(sx)=a(\alpha_x x)=\alpha_x(ax)=\alpha_x y.$$

所以 $\alpha_x=\alpha_y$. 即 $s=\alpha_x$，这就是说，s 是 F 中元. 于是定理成立.

下面是密度定理的逆.

定理 7 假定 V 是体 F 向量空间，R 是 V 的线性变换形成的环，如果 R 是 V 的 1 重可迁，那么 R 是本原环.

证明 假定 $v\neq 0$ 是 V 中任意元，因为 R 是 V 的 1 重可迁，所以 $Rv=V$. 命

$$M=\{r\mid r\in R, rv=0\},$$

显然 M 是 R 的左理想，并且 $M\neq R$. 于是 $(M:R)=0$，这是因为，如果 $r\in(M:R)$，由 $rR\subseteq M$ 得 $rRv=0$，即 $rV=0$，这就是说，r 把 V 中任意元变为 0，因此 $r=0$.

下面我们再证明 M 是 R 的极大左理想. 假定 R 的左理想 $N\supset M$，那么 R 中有元 $x\in N$，$x\overline{\in} M$，因此 $xv\neq 0$. 于是 $Rxv=V$，因为 $Rx\subseteq N$，所以 $Nv=V$. 即 $Nv=Rv$. 假定 r 是 R 中任意元，那么 N 中有元 n 使 $nv=rv$，即 $(n-r)v=0$，因此 $n-r\in M$，所以

$$r=n-m\in N,$$

这就是说，$R\subseteq N$，于是$R=N$，因此M是R的极大左理想.

于是R是本原环，定理得证.

要注意的是，这时R不一定是F空间V的稠密环，因为F不一定就是V的自同态环中所有与R中任意交换的元形成的体，一般它是包含F的体K的向量空间V的稠密环，因为R，F都可以看成在V的自同态环E中，所以$F\subseteq K$. 譬如V是复数域看成为实数域F的向量空间，R是V的线性变换形成的环，对于$0\neq v\in V$，显然$Rv=V$. 因此R是V的1重可迁，所以R是本原环. 但R不是F向量空间V的稠密环. 这是因为，$1,i$是V中对于F线性无关的元，并且R中不存在使$(a+bi)1=1$，$(a+bi)i=1$的元$a+bi$，所以R对于F的V不是2重可迁，因此R不是F的V的稠密环. 再我们容易得知，在V的自同态环中，所有与R中任意元能够交换的元形成的体是复数体C. 于是R是对于C的向量空间V的稠密环.

由上定理我们立即推得，假如R是向量空间V的线性变换形成的稠密环，那么R是本原环.

由密度定理，我们得到下面一个常常引用的关系.

定理8 假定R是本原环，那么有某体F，使得$R\simeq F_n$或对于任意正整数m，R有子环$S_{(m)}\sim F_m$.

证明 假定R是F向量空间V的稠密环，当V关于F的维数是n时，R是F向量空间V的所有线性变换形成的环，因此$R\simeq F_n$，当V关于F是无穷维时，假定$u_1,\cdots,u_m,\cdots$是无穷个线性无关的元，$V_m=Fu_1+\cdots+Fu_m$，因为R是稠密环，所以R中有把$u_1,\cdots,u_m$变为V_m中任意m个元的元，显然R中所有这样的元形成子环

$$S_{(m)}=\{x\mid x\in R, xV_m\subseteq V_m\},$$

并且它与F_m同态，即$S_{(m)}\sim F_m$. 定理证毕.

根据上面密度定理，我们不难得到下面本原环的两个性质.

定理 9　假定 R 是本原环，如果 R 中任意元的平方是 R 的左拟正则元，那么 R 是域.

证明　假定 R 是体 F 的向量空间 V 的稠密环，如果能够证明 V 的维数是 1，因为 1 维 F 向量空间的所有线性变换形成的环与 F 的中心同构，所以 R 就是域了.

假定 x,y 是 V 中任意两个线性无关的元，那么 R 中有元 a 使

$$ax=y, ay=-x,$$

即

$$a^2x=-x, a^2y=-y.$$

但 a^2 是 R 的左拟正则元，因此在 R 中有元 b 使得 $a^2+b+ba^2=0$，于是

$$(a^2+b+ba^2)x=a^2x+bx+ba^2x=-x,$$

即 $x=0$，这与 x,y 线性无关的假设矛盾. 也就是说，V 中任意两个元都线性相关，所以 V 的维数是 1. 于是定理成立.

定理 10　假定 R 是本原环，并且对于 R 中任意两元 a,b 有

$$a(ab-ba)=(ab-ba)a,$$

那么 R 是域.

证明　假定 x,y 是 V 中任意两个线性无关的元，那么 R 中有元 a,b 使

$$ax=y, ay=x+y, bx=y, by=x,$$

由计算得

$$a(ab-ba)x=x+y, (ab-ba)ax=-x.$$

于是 $x+y=-x$，即 $2x+y=0$ 这与 x,y 线性无关的假设不合. 因此 V 的维数是 1. 所以 R 是域，于是定理成立.

最后，介绍阿丁环的两个重要性质.

定理 11　本原阿丁环是单环.

证明　假如本原环 R 满足极小条件，如果我们能够证明

$$\overline{R}=R-M$$

是 F 的有穷维向量空间，那么定理就告成立. 证明用反证法.

假定 $\overline{R}$ 中有无穷个线性无关的元 $\overline{x}_i, i=1,2,\cdots$，因为 R 中所有零化 $\overline{x}_1,\cdots,\overline{x}_n$ 的元形成 R 的左理想 L_n，由定理 4，$L_i\neq L_j, i\neq j$. 于是 R 的左理想列

$$L_1\supset L_2\supset\cdots\supset L_n\supset\cdots$$

有无穷项，这与 R 满足极小条件的假设不合. 因此 F 空间 $\overline{R}$ 是有穷维的. 于是定理成立.

由 § 8.5 定理 13，我们容易得知阿丁单环又是本原环，因此，在阿丁环中，单环与本原环是一致的.

由 § 8.6 定理 2，我们得知半单环是本原环的次直和，假如环又是阿丁环，那么它就是 § 8.3 的定理 5. 下面另予直接证明.

定理 12 阿丁半单环是有穷个单环的直和.

证明 假定 R 是半单环，它与本原环 $\{R-N_i\}$ 的次直和同构，这里 $N_i(i=1,2,\cdots)$ 是 R 的理想. 因为 R 又满足极小条件，所以

$$N_1\supset N_1\cap N_2\supset\cdots$$

只有有穷项. 但 $\cap N_i=0$，因此我们有有穷个 N_i，譬如 $N_1,\cdots,N_n$，使 $\bigcap_{i=1}^{n}N_i=0$，而 $M_i=\bigcap_{j\neq i}N_j\neq 0$. 再由定理 11，本原环 $R-N_i$ 是单环，所以 N_i 是 R 的极大理想. 于是 $(N_i,M_i)=R$. 因为 $M_i\cap N_i=\cap N_i=0$，所以 $R=M_i+N_i$. 又因为 $M_i\simeq R-N_i$，所以 M_i 是单环. 我们命 $S_k=\bigcap_{i=1}^{k}N_i, k=1,\cdots,n$，于是 $R=M_1+N_1=M_1+S_1$. 如果我们能够证明，对于任意 $k<n$，$S_k=M_{k+1}+S_{k+1}$，因为 $S_n=0$，我们就得到 $R=M_1+\cdots+M_n$，即 R 是有穷个单环 M_i 的直和. 于是定理成立.

因为 $S_k\not\subseteq N_{k+1}$，而 N_{k+1} 是 R 的极大理想，所以 $R=(S_k, N_{k+1})$. 于是由第二同构定理（§ 6.2），

$$\begin{aligned}R-N_{k+1}&=(S_k,N_{k+1})-N_{k+1}\\&\simeq S_k-(S_k\cap N_{k+1})=S_k-S_{k+1},\end{aligned}$$

所以 S_k-S_{k+1} 是单环. 因此 S_{k+1} 是 S_k 的极大理想. 再因为

$$M_{k+1}\not\subseteq S_{k+1}, M_{k+1}\subseteq S_k,$$

所以 $S_k=(S_{k+1},M_{k+1})$，又因为 $S_{k+1}\cap M_{k+1}=0$，所以

$$S_k = M_{k+1} + S_{k+1}.$$

因此定理成立.

于是,贾柯勃逊根基是幂零根基最好的推广,得到的关于单环构造的密度定理也是魏特邦-阿丁第二构造定理最好的推广. 半单环的构造定理也是魏特邦-阿丁第一构造定理最好的推广,其中引为不足的是本原环远不及单环简单. 1947 年布朗(B. Brown)及麦珂把贾柯勃逊根基概念推广,建立了另一个根基概念,叫做布朗-麦珂根基[22]. 假如环 R 的布朗—麦珂根基是 G,那么 $\overline{R}=R-G$ 是有单位元的单环的次直和. 这结果与魏特邦-阿丁第一构造定理更为接近,但布朗-麦珂根基较贾柯勃逊根基复杂,不及贾柯勃逊根基自然,这是布朗-麦珂根基不足之处.

习 题 8.7

1. 假定 V 是体 K 的向量空间,R 是 V 的所有线性变换形成的环,那么 R 是 V 的稠密环.

2. 假定 G 是由(a,b)形成的加群,这里 $a,b\in F$,F 是实数域,$\alpha=(1,0)$,$\beta=(0,1)$,T 是 G 的自同态.

$$T\alpha=a_{11}\alpha+a_{12}\beta,\ T\beta=a_{21}\alpha+a_{22}\beta,$$

试证 G 的自同态环与全矩阵环 F_2 同构,$T\to\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$是它的同构映射.

3. 本原环是质环[17].

4. 本原环的中心是整环.

5. 假定 R 是本原环,$L=Re$ 是极小左理想,R 是体 F 的向量空间 V 的稠密环,试证 eV 关于 F 的维数是 1.

参 考 文 献

[1] J. H. M. Wedderburn, On hypercomplex numbers, Proc. London Math. Soc., 6(1908), 77～117.

[2] E. Artin, Zur Theorie der hyperkomplexen Zahlen, Abh. Math. Sem. Univ. Hamburg 5(1927), 251～260.

[3] N. Jacobson, The radical and semi-simplicity for arbitrary rings, Amer. J. Math. 67(1945),300～320.

[4] 谢邦杰、论根理想、吉林大学学报,第4期(1957),177～214.
N. J. Divinsky, Rings and Radicals(1965),116～156.

[5] N. Jacobson, Structure of rings(1956).

[6] I. N. Hersteion, On commutative Rings(1973).

[7] O. Barbara, Chain Conditions in Rings, Amer. Math. Monthly 85 (1978),771～772.

[8] C. Hopkins, Rings with minimal conditions for left ideals, Ann, of Math., V. 40(1939),712～730.
R. C. Shock, Nil subrings in finiteness Conditions, Amer. Math. Monthly 78(1971)741～748.

[9] R. Brauer, On the nilpotency of the radical of a ring, Bull. Amer. Math. Soc., V.48(1942),752～758.

[10] O. Goldman, A characterization of semi-simple ring with the descending Chain Condition, Bell. Amer. Math. Soc. (1946),1021.
D. W. Henderson, Ashort proof of Wedderburn's theorem. Amer. Math. Monthly, 72(1965),385～386.

[11] S. Perlis, A characterization of the radical of an algebra, Bull. Amer. Math. Soc., V. 48(1942),128～132.

[12] R. Steinberg, Dinision Ring, Amer. Math. Monthly, 58(1951),48.

[13] R. L. Kruse, On the circle group of a nilpotent ring, Amer. Math. Monthly, 77(1970),168～170.
J. C. Ault and J. F. Watters Circle groups of nilpotent Rings, Amer. Math. Monthly,80(1973),48～52.

[14] A. J. Goldman, Subring of a radical rings, Amer. Math. Monthly, 63(1956),350.

[15] R. V. Gopa, On primitivility of Matrix rings, Amer. Math. Monthly,75(1968),636～637.

[16] G. M. Bergman, A ring primitive on the right but not on the left. Proc. Amer. Math. Soc.,15(1964),473～475. Correction on page

1000.

[17] E. Sadiada; P. M. Cohen, An example of a simple radical rings ,J. algebra 5(1967). 373~377.

W. A. Mcworter. Some properties of simple nilrings, Can. Math. Bull,9(1966),199~200.

[18] R. N. Gupta, Primitive Simple rings, Amer. Math. Monthly,74 (1967),737.

[19] G. Birkhof, Subdirect unions in universal algebra, Bull. Amer. Math. Soc., 50(1944),764~768.

N. H. McCoy, Subdirect sums of rings, Bull. Amer. Math. Soc., 53(1947),856~877.

[20] Y. Adil, Elementery proofs of Commutative of p-rings, Amer. Math. Monthly, 64(1957),253~254.

[21] N. H. McCoy, Rings and Ideals, (1948),140~144.

[22] B. Brown, N. H. Mccoy, Radicals and subdirect sum. Amer. J. Math. 69(1947),46~58.

— —,The radical of a ring, Duke Math. J. 15(1948),495~499,

邱琦章,满足$[(XY)^m,(YX)^m]=0$的环. 武汉大学学报 1986 年第 3 期 9~14.

周尚超,关于诣覃环的一个问题,华中工学院学报,1983 年第 1 期 133~135.

熊全淹,环构造,湖北教育出版社(1984).

习 题 答 案

习题中除个别认为较简单的外，都给出解答，但解答非常简略，只作为解题思路，供读者参考校核而已.

习 题 1.1

1. 任意两个集都有交集与并集.

2. $A\cup B=B, A\cap B=A$.

5. i 元集有 C_n^i 个，空集 1 个，共有子集

$$C_n^0+C_n^1+\cdots+C_n^n=(1+1)^n=2^n.$$

习 题 1.2

2. 这时整数集分为 5 类：$\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$.

3. 如果 τ 有逆 τ^{-1}，那么 $\sigma=\tau^{-1}$. 再假如 $\tau(x_1)=y_1,\tau(x_2)=y_2$，如果 $y_1=y_2$，那么 $\sigma\tau(x_1)=\sigma\tau(x_2)$，即 $x_1=x_2$. 于是 τ 是可逆的，所以有逆.

5. 假如不存在使 $a\sim b$ 的 b，那么 $a\sim a$ 就不能成立.

习 题 2.1

1. 没有单位元，所以不成群；又因为 $(2\circ 3)4\neq 2(3\circ 4)$，所以结合律也不成立.

2. 成为群，群表为

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

这里 $a=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $b=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$, $c=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $d=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$.

3. 群表为

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	d	c	f	e
c	c	e	a	f	b	d
d	d	f	b	e	a	c
e	e	c	f	a	d	b
f	f	d	e	b	c	a

$a=r, b=\frac{1}{r}$,

$c=1-r, d=\frac{1}{1-r}$,

$e=\frac{r-1}{r}, f=\frac{r}{r-1}$.

4. 空集是单位元，A 的逆是 A 自身.

5. $s^2=(ae)(bc), t^2=(acb), st=(aedcb)$

$ts=(acbde), tst^{-1}=(abcd), sts^{-1}=(abe)(cd)$.

6.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	5	1	6	2	4
4	4	6	5	1	3	2
5	5	3	4	2	6	1
6	6	4	2	3	1	5

这里 $1=(1), 2=(12)$,

$3=(13), 4=(23)$,

$5=(123), 6=(132)$.

即 $S_3=\{1, 5, 5^2(=6), 4, 5\cdot 4(=2), 5^2\cdot 4(=3)\}$.

7. 因为 $(ab)^2=abab=a^2b^2$，所以 $ba=ab$.

8. 由 $abab=e$ 得 $bab=a$，因此 $ba=ab$.

9. 因为 G 是非交换群，所以其中存在 $a^{-1}\neq a$ 的元 a，命 $b=a^{-1}$，那么

$$ab=ba.$$

10. 由 $ax=b$ 在 G 中有解及消去律得知 σ_a 是可逆映射. 再因为 $\sigma_a\sigma_b(g)=\sigma_a(bg)=abg=\sigma_{ab}(g)$，所以 $\sigma_a\sigma_b=\sigma_{ab}$.

11. 由 3°, $e/(b/c)=c/b$，因此我们有 $(ac^{-1})(cb^{-1})=ab^{-1}$，命 $a=x, b=e, c=y^{-1}$，即得 $x=xe^{-1}=(xy)(y^{-1}e^{-1})=(xy)y^{-1}$. 又命 $a=xy, b^{-1}=z, c=y$ 得结合律 $(xy)z=((xy)y^{-1})(yz)=x(yz)$.

习 题 2.2

2. $\mathbf{Z}-(100)=(\bar{1}),(\bar{2}),(\bar{4}),(\bar{5}),(\overline{10}),(\overline{20}),(\overline{25}),(\overline{50}),(\overline{100})=(\bar{0})$.

3. 假定 a^m 的阶数是 k，即 $a^{mk}=e$，那么 $n\mid mk$，因此 $\frac{n}{(n,m)}\Big|\frac{m}{(n,m)}k$. 但 $\frac{n}{(n,m)}$，$\frac{m}{(n,m)}$ 互质，所以 $\frac{n}{(n,m)}\Big|k$. 再 $(a^m)^{\frac{n}{(n,m)}}=(a^n)^{\frac{m}{(n,m)}}=e$，所以 $k\Big|\frac{n}{(n,m)}$，因此，$k=\frac{n}{(n,m)}$.

4. 设乘积 ab 的阶数是 r. 因为 $a^m=1, b^n=1$，所以 $(ab)^{mn}=1$，因此 $r\mid mn$. 再因为 $(ab)^{mr}=b^{mr}=1$，$(ab)^{nr}=a^{nr}=1$，所以 $n\mid mr, m\mid nr$. 如果 $(m,n)=1$，那么 $n\mid r, m\mid r$，因此 $mn\mid r$，所以 $r=mn$.

又假如 $m=p_1^{t_1}p_2^{t_2}p_3^{t_3}$，$n=p_1^{s_1}p_2^{s_2}p_3^{s_3}$，$t_1\geqslant s_1$，$t_2\leqslant s_2$，$t_3\geqslant s_3$，于是 $q=p_1^{t_1}p_2^{s_2}p_3^{t_3}$. 但 $a^{p_2^{t_2}}$ 的阶为 $p_1^{t_1}p_3^{t_3}$，$b^{p_1^{s_1}p_3^{s_3}}$ 的阶为 $p_2^{s_2}$，所以 $a^{p_2^{t_2}}\cdot b^{p_1^{s_1}p_3^{s_3}}$ 的阶为 q.

5. 假如 $a^m=1, b^n=1$，如果 $n\nmid m$，那么 m,n 的最小公倍 $q>m$，于是 G 中有阶为 q 的元，这与假设不合.

8. 因为任意排列可以写成循环排列的乘积，并且

$$(12\cdots n)=(1n)(1n-1)\cdots(12),\quad (ij)=(1i)(1j)(1i).$$

9. 因为 $(1j)(1i)=(1ij)$，$(1ij)=(12j)^2(12i)(12j)$.

10. 假定 $A\nsubseteq B, B\nsubseteq A, a\in A-B, b\in B-A$. 如果 $ab\in A$，那么 $a^{-1}(ab)=b\in A$，此与假设不合，因此 $ab\notin A$. 同样 $ab\notin B$. 所以 $A\cup B$ 不成群.

11. 设 n 是奇数，a 是 G 中任一异于 e 的元，那么 a 的阶数是奇数 n 的因数，因此也是奇数，设为 $2k-1$，即 $a^{2k-1}=e$，所以 $a^{2k}=a$，因此 a 是 a^k 的平方. 假如 n 是偶数，那么 G 中除 e 外有奇数个元，因此至少有一个元它的逆就是它自身. 于是在群表的对角线上 e 至少出现 2 次，所以有某元 y 不出现，因此 y 不是某元的平方.

习 题 2.3

1. $a\in G, a\neq e$ 时，(a) 的元数是 G 的元数的因数，因此 $G=(a)$.

2. 对于任一不在 H 中的 a，$G=H\cup aH$，$G=H\cup Ha$，所以 $aH=Ha$.

3. $G=a_1H\cup a_2H\cup\cdots$，$H=b_1K\cup b_2K\cup\cdots$ 时，如果 $a_ib_jK\cap a_hb_lK\neq 0$，那

么 $a_ib_j=a_hb_lk$，于是 $a_i=a_hb_lkb_j^{-1}\in a_hH$，所以 $a_i=a_h$，因此 $b_j=b_l$，即 $i=h$，$j=l$. 或 $|K|\cdot|G:K|=|G|=|H|\cdot|G:H|=|K|\cdot|H:K|\cdot|G:H|$.

4. 假定 $G=(a)$，$H=(a^r)$，于是 $G=H\cup aH\cup\cdots\cup a^{r-1}H$. 所以 $(G:H)=r$.

5. 当 $aH\cdot bH=abH$ 时，$ahb=abh_1$，因此 $bh_1b^{-1}\in H$.

6. 因为 $h^{-1}k^{-1}(hk)=h^{-1}(k^{-1}hk)=(h^{-1}k^{-1}h)k\in H\cap K$.

10. $G^2=\{\pm1\}$，$G^3=G$，$G^4=\{1\}$.

11. A_4的子群中 2 元的有 3 个：

$$\{(1),(12)(34)\}=((12)(34)),$$
$$\{(1),(13)(24)\}=((13)(24)),$$
$$\{(1),(14)(23)\}=((14)(23));$$

3 元的有 4 个：

$$((123))=((132)),\quad ((124))=((142)),$$
$$((134))=((143)),\quad ((234)=((243));$$

4 元的只有 1 个：

$$B_4=\{(1),(12)(34),(13)(24),(14)(23)\}.$$

它没有 6 元子群，只有 B_4 是正规子群.

12. 因为 $B_4\lhd A_4$，又 A_4/B_4 是交换群，所以 $D(A_4)\subseteq B_4$. 但 A_4 只有 B_4 是正规子群，其它子群都不是正规子群，所以 $D(A_4)=B_4$.

13. 假如 $\tau(i)=j$，$i\neq j$ 时，有适当的 σ 使 $\sigma\tau\sigma^{-1}(i)\neq j$，那么 S_n 的中心就是单位元群. 取 $\sigma=(j,k)$，$k\neq j,i$，显然 $\sigma\tau\sigma^{-1}(i)=k$，$i\neq k$.

14. 假设 $H\lhd S_4$，$H\neq S_4$，$H\neq A_4$，$H\neq$单位元群，那么

(i) H 不包含奇排列(12)，(13)，(14)，(23)，(24)，(34)，(1234)，(1243)，(1324)，(1342)，(1423)，(1432). 这是因为如果 H 包含(12)，那么它也包含(23)(12)(23)=(13)，(24)(12)(24)=(14)，于是 $H=S_4$. 又如果 H 包含(1234)，那么它也包含(12)(1234)(12)=(1342). 同样它又包含其余 4 个(1243)，(1324)，(1423)，(1432). 于是它包含(1234)$(1243)^2$=(24)，再加上单位元，H 最少包含 13 个元，因此 $H=S_4$.

(ii) H 不包含偶排列(123)，(132)，(124)，(142)，(134)，(143)，(234)，(243). 这是因为如果 H 包含(123)，它也包含(34)(123)(34)=(124)，因此 $H\supseteq A_4$.

(iii) $H=\{(1),(12)(34),(13)(24),(14)(23)\}$，这是因为由 §2.2 习题

10，两个对换的积的共轭仍为两个对换的积，但 S_4 中两个对换的积只有上面三个．因此 $H\lhd S_4$.

15．假如 $H\lhd S_n(n>4)$，因为 $(H\cap A_n)\lhd A_n$，所以 $H\cap A_n=A_n$ 或 $H\cap A_n$ ＝单位元群．从前者言，$H\supseteq A_n$．从后者言，H 所包含的元除单位元外都是奇排列，并且它们的平方又都是单位元．再这些奇排列用不同文字的循环排列的乘积表示时又都是对换的乘积，因为不如此，它的平方就不是单位元．又 H 不含两个奇排列，因为两个这样奇排列的乘积是单位元，于是它们互逆，因此它们就相等．假如 $s=(ij)\cdots$ 是 H 所含的奇排列，命 $t=(ik),k\neq j$，那么 $tst^{-1}=(kj)\cdots\in H$，这不可，所以 H 是单位元群.

习 题 2.4

1．因为 G 是交换群，所以除恒等同构外没有内同构．外同构有五：(ab)，(bc)，(ca)，(abc)，(acb)．由群表得知 a,b,c 中任意二元的乘积等于第三元，所以上面 5 个单射都是同构.

2．n 元群如果它的中心是单位元群，那么它有 n 个互异的内同构，因为 S_3 的中心是单位元群，所以它有六个内同构.

再因为 $(123)=(12)(23)$，$(132)=(13)(32)$，所以 S_3 是由 (12)，(13)，(23) 生成的群．因此 S_3 的任一自同构把 (12)，(13)，(23) 互换，两个不同的自同构有不同的互换，于是 S_3 最多只能有六个自同构，所以它没有外同构.

3．因为命 $\pm 1=\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$\pm i=\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}$，$\pm j=\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}$，$\pm k=\pm\begin{pmatrix}0&i\\i&0\end{pmatrix}$ 时，§2.3 习题 8 中各关系成立.

4．因为 $H\cap K$ 是 G 的子群，$H\cap K\subseteq K$，所以 $H\cap K$ 是 K 的子群．再如果 $a\in H\cap K$，$k\in K$，那么 $kak^{-1}\in H$，$kak^{-1}\in K$，所以 $kak^{-1}\in H\cap K$.

5．因为 $\overline{gkg}^{-1}=\bar{k}'$，即 $\overline{gkg}^{-1}=\bar{k}'$，所以 $gkg^{-1}=k'h$，因此 $gkg^{-1}\in K$.

6．假如有穷群 G 是它的子群 H 的所有共轭子群的并集，那么 H 的共轭子群的个数是 1，因此 $H=G$．这是因为，如果 H 的共轭子群的个数大于 1，因为子群的单位元都相同，所以 G 的元数就小于 H 的元数与它的共轭子群的个数的乘积，因此 H 在 G 的指标就小于 H 的共轭子群的个数，这显然是矛盾.

7．由群方程 $p^n=a_0+a_1p+a_2p^2+\cdots$，得知 $a_0\neq 1$.

8. 假如 G 的中心 Z 的元数是 p，命 a 是 G 中不在 Z 中的元，那么 G 中所有与 a 能够交换的元形成的群就是 G. 因此 $a\in Z$，这与假设不合.

9. 假定 $\sigma_a(x)=axa^{-1}$，如果 $\sigma_a=\sigma_b$，那么 $b^{-1}ax=xb^{-1}a$，因为 G 的中心是单位元群，所以 $b^{-1}a=e$，于是 $a=b$.

10. 假如 c 是中心 Z 中任一元，g 是 G 中任一元，如果 $c\to c'$，$g'\to g$，因为 $g'c=cg'$，所以 $gc'=c'g$ 于是 $c'\in Z$；再

$$\sigma[x,y]=\sigma(x^{-1}y^{-1}xy)=(\sigma x)^{-1}(\sigma y)^{-1}\sigma(x)\sigma(y)=[\sigma(x),\sigma(y)].$$

11. 由 $A\supseteq B\supseteq C$ 及 σ 是 A 的自同构，得 $\sigma(B)\subseteq B$，如果 $\sigma(B)\subset B$，命 $b'\in B$ 但 $\in\sigma(B)$，b' 的象源是 b，显然 $b\overline{\in}B$. 所以 σ^{-1} 把 $b'\to b$，这与 B 是特征子群的假设不合. 于是 $\sigma(B)=B$. 因此 σ 又是 B 的自同构，所以 $\sigma(c)\subseteq C$.

12. 因为 $H\supseteq G'$，$ghg^{-1}h^{-1}\in H$，所以 $ghg^{-1}\in H$，即 $gHg^{-1}\subseteq H$.

15. 设 $G=\{1,a,b,c\}$，如果 G 不是循环群，那么 $a^2=b^2=c^2=1$，因此 $ab=c$，$bc=a$，$ca=b$，即 G 是克莱茵 4 元群.

16. 设 6 元群 G 不是循环群，那么 G 中元的阶不是 2 便是 3，我们容易验证 G 中元的阶不能都是 2，因此 G 中必有阶为 3 的元，设 $a^3=1$，a，a^2 都在 G 中，再设 b 是 G 中其它任一元，那么 $1,a,a^2,b,ab,a^2b$ 是互异的 6 个元，因此 $G=\{1,a,a^2,b,ab,a^2b\}$，这就是 S_3 即 $G=S_3$.

17. 设 G 是 8 元非交换群，其中元不能全部都是阶数为 2 的元，也没有阶数为 8 的元，因此 G 有阶数为 4 的元，设 $a^4=1$，所以 $(a)\lhd G$. $\overline{G}=G/(a)=(\overline{b})$，$\overline{b}^2\in(a)$. 于是 $G=\langle a,b\rangle$，其中 $a^4=1$，$b\overline{\in}(a)$，$b^2\in(a)$，因为 b 的阶不能为 8，所以 $b^2=1$ 或 $b^2=a^2$. 于是 $G=\langle a,b\rangle$ 其中 $a^4=1$，$b^2=1$，$b^{-1}ab=a^3$ 或其中 $a^4=1$，$b^2=a^2$，$b^{-1}ab=a^3$. 前者是二面体群，后者是四元数群.

18. 因为 $S_4=A_4\cup(12)A_4=H\cup(123)H\cup(132)H\cup(142)H\cup(12)H\cup(23)H\cup(13)H\cup(14)H$，而 (123)，(132)，(142)，(12)，(23)，(13)，(24) 中只有 (23) 能够与 H 交换，所以 H 的正规化子 $K=H\cup(23)H$，再因为 $S_4=K\cup(123)K\cup(132)K\cup(142)K$. 于是它的共轭子群是

$$H=\{(1),(234),(243)\},(123)H(132)=\{(1),(143),(134)\},$$
$$(132)H(123)=\{(1),(124),(142)\},$$
$$(142)H(124)=\{(1),(132),(123)\}.$$

19. 引用 § 2.2 的计算，得知 (12)，(34) 互为共轭，(13)(24)，(14)(23) 互为 共轭，(1324) 与 (1423) 互为共轭，(13)(24) 自己共轭，因此 B_8 的中心为 $\{(1),(12)(34)\}$，正规子群有

$$\{(1),(12),(34),(12)(34)\},$$

$$\{(1),(12)(34),(13)(24),(14)(23)\},$$

$$((1423))=((1324))=\{(1),(12)(34),(1423),(1324)\}.$$

20. S_4 的 3 元子群 4 个：

$$\{1,(234),(243)\},\{1,(341),(314)\},$$

$$\{1,(412),(421)\},\{1,(123),(132)\}$$

它们彼此共轭，8 元子群 3 个：

$$B_8,(13)B_8(13),(14)B_8(14)$$

它们也显然共轭.

习 题 2.5

1. 因为 $S_4=A_4\cup(12)A_4$，$A_4=B_4\cup(123)B_4\cup(132)B_4$，所以 $S_4=B_4\cup(12)B_4\cup(13)B_4\cup(23)B_4\cup(123)B_4\cup(132)B_4$. 因此

$$S_4/B_4\cong\{(1),(12),(13),(23),(123),(132)\}.$$

3. 假定 $\sigma_a(g)=aga^{-1}$，如果 $\sigma_a=1$，那么 $aga^{-1}=g$，即 $ag=ga$，所以 $a\in Z$，因此同态核是 Z.

5. 假定 $G\sim G'$，同态核是 E，H' 是 G' 的子群，H 是 H' 在 G 的完全象源，于是 $H'\simeq H/E$.

6. 假定 $G/Z=(\bar{a})$，那么 $G=\bigcup a^iZ$，因此 a^iZ 中任意元能够与 a^jZ 中任意元交换，所以 G 是交换群.

8. 设 $a_1,\cdots,a_n$ 是 G 中 n 个元，因为 $\bar{G}=G/N$ 是局部有穷，所以由 $\bar{a}_1,\cdots,\bar{a}_n$ 生成的子群是有穷的. 设为 $\{\bar{a}_1,\cdots,\bar{a}_n,\bar{a}_{n+1},\cdots,\bar{a}_m\}$，因为 $\bar{a}_i\bar{a}_j=\bar{a}_l$，所以 $a_ia_j=u_{ij}a_l$，$u_{ij}\in N$. 因此 $a_ia_ja_k=u_{ij}a_la_k=u_{ij}u_{lk}a_h$，一般 $a_{i1}a_{i2}\cdots a_{it}=u_ia_l$，于是由 $a_1,\cdots,a_n$ 生成的子群其元数 不大于由 u_{ij} 生成的 N 的子群的元数与 m 的乘积，因此是有穷群.

9. $a\to a^{-1}$ 是逆同构映射.

习 题 3.1

1. 分配律不成立.

2. 成环，$(1,1)$ 是单位元，$(0,0)$ 是零元，$(a,0)$，$(0,b)$ 都是零因子，(a,b) 的逆元是 (a^{-1},b^{-1}).

4. $(a+b)(e+e)=(a+b)e+(a+b)e=(a+b)+(a+b)$

$$=a+(b+(a+b))$$

又 $$=a(e+e)+b(e+e)=(a+a)+(b+b)$$

$$=a+(a+(b+b))$$

所以 $b+(a+b)=a+(b+b)$，即$(b+a)+b=(a+b)+b$.

因此 $a+b=b+a$.

6. 假如 $ab=0, b\neq 0$ 时，如果有 a_R^{-1}，因为 $aa_R^{-1}+ab=a(a_R^{-1}+b)=e$，所以 $a_R^{-1}+b$ 又是 a 的右逆.

7. 设 $a^m=a^n, m<n$，那么 $a^{m-1}(a-a^{n-m+1})=0$，因为 a 不是零因子，所以 $a=a^{n-m+1}$. 再因为 $ba=ba^{n-m+1}$，所以$(b-ba^{n-m})a=0$，于是 $b=ba^{n-m}$. 因此 a^{n-m}是单位元，由 $a\cdot a^{n-m-1}=a^{n-m}$，所以 a 是可逆元.

8. 因为$(r-re)e=0$.

9. 假定 E_{ij}是 i 行 j 列的元是 1，其余元都是 0 的方阵，因为$(a_{ij})E_{ij}=E_{ij}(a_{ij})$，所以 $\begin{pmatrix} \vdots & a_{1i} & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & a_{ni} & \vdots \end{pmatrix}=\begin{pmatrix} \cdots\cdots\cdots \\ a_{j1}\cdots a_{jn} \\ \cdots\cdots\cdots \end{pmatrix}$，于是 $a_{ki}=a_{jk}=0, a_{ii}=a_{jj}=a$，因此 $(a_{ij})=\mathrm{diag}(a,\cdots,a)$.

10. 假如 $a^2=a, r\in R$，因为$(ara-ar)^2=0$，所以 $ara=ar$. 同样 $ara=ra$，于是 $ar=ra$.

11. 由 $4a^2=2a$，我们有 $2a=0$，即 $a=-a$. 又由$(a+b)^2=a+b$，得 $ab+ba=0$，所以 $ab=ba$.

习 题 3.2

1. $Z-(2)$.

2. 譬如$\bar{2},\bar{3}$都是 $Z-(6)$的零因子.

3. 因为适当取$(ae-bi-cj-dk)(ae+bi+cj+dk)=(a^2+b^2+c^2+d^2)e$ 中的复数 a,b,c,d 可使 $a^2+b^2+c^2+d^2=0$，所以这时 $ae+bi+cj+dk$ 是右零因子.

4. 因为是有穷群，由消去律即得.

6. 因为 $t=ab-ba$ 的实数部分为零，设 $t=bi+cj+dk$，显然$(-bi-cj-dk)(bi+cj+dk)=b^2+c^2+d^2$，即$-tt=-t^2$ 是实数.

习 题 3.3

1. 因为 R 是加群，$R\sim S$，所以 S 也是加群. 再 S 中结合律，分配律可以与§2.5 定理1的证明类似证明. 所以 S 成环. 又因为乘群的同态象仍然是乘群，所以当 R 是体时，S 也是体.

3. 如果同构，那么 $0\to e$. 设 $a\to -e$. 于是 $2a\to e$. 所以 $2a=0$，因此 $2e=0$. 再设 $e\to b$，那么 $b^2=e$，因为 $b^2-e^2=(b-e)(b+e)=0$，所以 $b=e$，即 $e\to e$ 此不可.

4. 因为有理数显然变为自身，如果 $i\to j$，由 $i^2=-1$ 得 $j^2=-1$，因此 $i^2=j^2$，所以 $i=j$ 或 $i=-j$，即 $i\to i$ 或 $i\to -i$.

5. 假如 $1\to a$，那么 $2\to 2a$，如果 $\frac{1}{2}\to b$，由 $1\to 2b$ 得 $a=2b$ 即 $b=\frac{a}{2}$. 也就是说，当 $1\to a$ 时，$\frac{1}{2}\to\frac{1}{2}a$.

6. 因为 $e\to\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$i\to\begin{pmatrix}i&0\\0&-i\end{pmatrix}$，$j\to\begin{pmatrix}0&1\\-1&0\end{pmatrix}$，$k\to\begin{pmatrix}0&i\\i&0\end{pmatrix}$. 即

$$ae+bi+cj+dk\to\begin{pmatrix}a+bi&c+di\\-c+di&a-bi\end{pmatrix}$$

是同构映射，所以它们成为体.

9. 假定环 R,S 的加群分别是由 x,y 生成的 n 阶循环群，并且 $x^2=kx,y^2=ly$，我们不难证明 $x\to ry$ 是 R 到 S 的同构，其必要充分条件是 $(r,n)=1,rl\equiv k(\mathrm{mod}\,n)$，也就是 $(k,n)=(l,n)$. 所以 n 阶循环环不同型的个数等于 n 的正约数的个数 $T(n)$.

10. 假定 R 的单位元 e（看成加群中元）的阶数是 m，那么 $R\simeq Z-(m)$. 因此两环同构，假如 e 的阶数 n，$1<n<m$，那么 $m=m'n,m'>1$，设 p 是 m' 的质约数，那么在 R 中最少有一元 a 使 $pa=0$，因为 $na=ne\cdot a=0\cdot a=0$. 所以 $p|n$，于是 $p^2|m$，这与假设矛盾.

习 题 3.4

1. 有理数域包含这整环，而有理数域没有异于自身的子体，所以它的分式域就是有理数域.

3. $(0,1)$ 是单位元，所有形如 $(a,0)$ 的元成为与 R 同构的环，所有形如 $(0,m)$ 的元成为与 Z 同构的环.

习 题 3.5

1. 当R是无零因子环时，m次多项式与n次多项式的乘积就是$m+n$次多项式.

2. 因为$R[x]$中次数大于零的多项式$f(x)$不可能有逆元.

4. $q(x)=\begin{pmatrix}2 & 0\\ 2 & 0\end{pmatrix}x-\begin{pmatrix}2 & 4\\ 2 & 4\end{pmatrix}, r=\begin{pmatrix}-5 & 9\\ -6 & 9\end{pmatrix}$;

$q_0(x)=\begin{pmatrix}2 & 0\\ 2 & 0\end{pmatrix}x-\begin{pmatrix}6 & 0\\ -2 & 0\end{pmatrix}, r_0=\begin{pmatrix}3 & 1\\ -14 & 1\end{pmatrix}$.

习 题 3.6

1. 所有形如$4r$的整数在整数环中形成主理想(4)，但在偶数环中组成的不是主理想(4)而是(8).

4. 因为$\bar{e}_1\bar{a}=\bar{a}, \bar{a}\bar{e}_2=\bar{a}$，即$\bar{e}_1, \bar{e}_2$分别是$\bar{R}=R-N$的左、右单位元，所以$\bar{e}_1=\bar{e}_2$是$\bar{R}$的单位元.

5. 在$Z[x]$中，假如$(x,2)=(f(x))$，那么$x=rf(x), 2=sf(x)$. 于是$f(x)=2$，因此$r=\frac{1}{2}x\bar{\in} Z[x]$.

7. 因$f(x)=(x^2+1)q(x)+a+bx, \bar{f}(x)=\bar{a}+\bar{b}\,\bar{x}$，所以$a+bi\to\bar{a}+\bar{b}\,\bar{x}$是它们的同构映射.

8. 因为$S\sim S'$的同态核$M\subseteq S$，又$M\subseteq N$，所以$M\subseteq S\cap N=0$.

9. 假定$\bar{A}$是$Z-(p^n)$中非零理想，$\bar{0}\neq\bar{a}\in\bar{A}$，那么$a\not\equiv 0(p^n)$，但$(a,p^n)=p^l, l<n$，所以$p^l=ra+sp^n$，因此$\bar{p}^l=\bar{r}\,\bar{a}+\bar{s}\bar{p}^n=\bar{r}\,\bar{a}\in\bar{A}$.

10. 假定R中所有形如$ra^n, r\in R$，的元组成的理想是A_n，因为$A_1, A_2, \cdots, A_n, \cdots$中必有相同的，命$A_m=A_n, m<n$，那么$ba^m=ra^n$，于是$b=a(ra^{n-m-1})$，因此$ax=b$在$R$中有解.

11. 假定R有单位元1，那么中心$Z\neq 0$. 命$c\in Z$，因为Rc是R的理想，并且$Rc\neq 0$，所以$Rc=R$，因此$c'c=1$即$c'=c^{-1}$. 又因为$c'r=c'r\cdot 1=c'r\cdot cc'=c'c\cdot rc'=rc'$. 所以$c'\in Z$.

再假如R的中心$Z\neq 0$. 命$c\in Z$，因为$Rc=cR$，如果$Rc=0$，那么(c)就是R中异于零的理想，于是$(c)=R$这与R不是幂零环的假设不合，所以$Rc=R$，因此$ec=ce=c$. 如果$rc=b$，那么$eb=erc=ecr=cr=b$. 所以e是R的单位

元.

12. 设 N 是 RL 的非零理想，因为 R 是单环，所以

$$RL=(RLNR)L=(RL)N(RL)\subseteq N.$$

因此 $N=RL$，即 RL 是单环. 再假如 RL 有单位元 e，那么对任意 $r\in R$ 由 $re^2=re$ 就有 $re=r$. 因此 $R=Re\subseteq RL\subseteq L$，这与 L 是 R 的真理想的假设矛盾，所以 RL 没有单位元.

13. 假定 $RxR=R$，设 $0\neq A$ 是 R 的理想，$x\in A$，那么

$$R=RxR\subseteq A$$

所以 $A=R$，因此 R 是单环. 反过来，假如 R 是单环，

$$A=\{x\mid x\in R,RxR=0\}$$

是 R 的理想，如果 $A=R$，那么 $R^3=0$，这与 R 非幂零的假设矛盾. 所以 $A=0$. 于是 $x\neq 0$ 时 $RxR\neq 0$，因此 $RxR=R$.

14. 假定 $x\in L$，$r\in R$ 是 $1+x$ 的左逆元，即 $r(1+x)=1$，所以 $r=1-rx\in 1+L$，因此有 r' 使 $r'r=1$，于是 $1+x=r'r(1+x)=r'$，即 $(1+x)r=r'r=1$. 所以 r 又是 $1+x$ 的右逆元.

15. 假定 $0\neq N$ 是 eRe 的理想，显然 RNR 是 R 的理想并且 $RNR\neq 0$. 因此 $RNR=R$. 于是

$$M2(eRe)N(eRe)=e(RNR)e=eRe$$

所以 $N=eRe$. 即 eRe 是单环.

16. 1) 因为 $aa'a=a$，设 $e=a'a$，显然 $e^2=e$，再因为 $Ra'\subseteq R$，所以 $Ra'a\subseteq Ra$，即 $Re\subseteq Ra$，又 $Ra\subseteq R$，所以 $Raa'a\subseteq Ra'a$，即 $Ra\subseteq Re$，因此 $Ra=Re$.

2) 设 $Ra=Re$，$Rb\subseteq Rbe+R(b-be)$，于是

$$Ra+Rb=Re+R(b-be)$$

设 $R(b-be)=Rf$，这里 $f^2=f$，并且 $fe=0$，设 $g=f-ef$，由计算得

$$fg=f,gf=g,g^2=g,eg=ge=0,$$

又因为 $g\in Rf$，$f\in R_g$，所以 $Rf=Rg$. 于是

$$Ra+Rb=Re+Rf=Re+Rg,$$

因为 $re+r'g=(re+r'g)(e+g)$，所以 $Re+Rg\subseteq R(e+g)$，反过来显然成立，所以 $Re+Rg=R(e+g)$. 这里 $e+g$ 是幂等元.

习 题 3.7

1. $(6):(3)=(2)$，$(6):(5)=(6)$，$(3):(9)=R$.

3. (i)→(iii), $A:BC=(A:B):C=A:C=A$. (iii)→(ii), 因为 $BC\subseteq B\cap C$, 所以 $A:(B\cap C)\subseteq A:BC=A$, 因此 $A:(B\cap C)=A$. (ii)→(i), 因为 $B\cap C\subseteq B$, 所以 $A:B\subseteq A:(B\cap C)=A$, 因此 $A:B=A$.

5. 因为 $(A,B)=R$, $(A,C)=R$, 所以 $R=(A,B)(A,C)=(A^2,AC,BA,BC)\subseteq(A,BC)$, 所以 $(A,BC)=R$.

6. 因为 $(A,B)=R$ 时, $AB=A\cap B$, 再因为 $(A,B)=R$, $(A,C)=R$ 时, $(A,BC)=R$, 所以 $ABC=A\cap BC=A\cap B\cap C$.

习 题 3.8

1. 因为 $Q[x]-(x)\simeq Q$, 所以 (x) 是极大理想.

2. 因为 $Z[x]-(x)\simeq Z$, 所以 (x) 是质理想, 又因为 $Z(x)-(2,x)\simeq Z-(2)$, 所以 $(2,x)$ 是极大理想.

3. 假定 $(a+bi)(c+di)\equiv 0(3)$, 那么 $(a^2+b^2)(c^2+d^2)\equiv 0(3)$, 但当 $a^2+b^2\equiv 0(3)$ 时 $a\equiv 0, b\equiv 0$, 因为 $a\neq 0$ 时 $a^2\equiv 1$. 所以 (3) 是质理想.

又因为 $2=(1-i)(1+i)\equiv 0(1+i)$, $1-i=(1+i)(-i)\equiv 0(1+i)$, 所以 $a+bi\equiv a+b\equiv 0$ 或 1. 于是 $Z[i]-(1+i)=\{\bar{0},\bar{1}\}\simeq Z-(2)$, 因此 $(1+i)$ 是极大理想.

5. 因为 $P\neq A$, 所以 $P\subset A$. 命 $p\in P$, $a\in A$, $a\overline{\in}P$, r 是 R 中任一元, 因为 $ra\in A$, 所以 $ra\cdot p=a\cdot rp\in P$, 因此 $rp\in P$.

6. 假定 N 是 R 的极大理想, 如果 $A\nsubseteq N$, $B\nsubseteq N$, 那么 $(N,A)=R$, $(N,B)=R$, 于是 $(N,A)(N,B)=(N,AB)=R$, 所以 $AB\nsubseteq N$.

8. 假定 P 是质环, $aRb\subseteq P$, 那么 $(RaR)(RbR)\subseteq P$, 因此 $RaR\subseteq P$ 或 $RbR\subseteq P$, 如果 $RaR\subseteq P$, 设 $A=(a)=\{ra+as+\Sigma u_iav_i+na\}$, 我们容易验证 $A^3\subseteq RaR$, 因此 $A\subseteq P$, 所以 $a\in P$. 反过来, 假如 $AB\subseteq P$, $A\nsubseteq P$, 设 $a\in A$, $a\overline{\in}P$, 因为对于任意 $b\in B$, $aRb\in P$, 由充分条件 $b\in P$, 所以 $B\subseteq P$ 即 P 是质环.

9. 必要条件由定理 1 的充分条件证法即得. 充分条件用定理 1 的必要条件的证法, 其中以 ar 形成的理想 A 代替 (a), 因为 $\bar{a}\neq 0$. 所以 $a^2\not\equiv 0(N)$, 于是 $N\subset(A,N)$, 因此 $(A,N)=R$.

10. 假定 R 的单位元是 e, 显然 R 的真理想不包含 e, 在 R 的所有真理想集合中, 我们有 $N_0\subset N_1\subset\cdots\subset N_n\subset\cdots$, 那么它们的并集不包含 e, 因此它就是所求的极大理想.

习 题 3.9

1. 因为 $Z-(19)$ 成体，所以 $6x\equiv17(19)$ 有解. 显然 $x=6$ 是它的解.

2. 假如 $(a+b\sqrt{-5})(c+d\sqrt{-5})=3$ 或 $2+\sqrt{-5}$，那么

$$(a^2+5b^2)(c^2+5d^2)=9,$$

于是

$$\begin{cases}a^2+5b^2=3\\c^2+5d^2=3\end{cases}\text{或}\begin{cases}a^2+5b^2=9\\c^2+5d^2=1\end{cases}$$

前者不可能，后者 $c=1,d=0$，因此 $c+d\sqrt{-5}=1$ 是单位元.

3. 因为 b,c 与 a 互质时，bc 也与 a 互质. 又当 b 与 a 互质时，$ra+sb=1$. 于是 $\bar{r}\,\bar{a}+\bar{s}\,\bar{b}=\bar{1}$，所以 $\bar{s}\,\bar{b}=\bar{1}$.

4. 假定对于 $\alpha=a+bi$，命 $\sigma(\alpha)=a^2+b^2$. $\beta=c+di$，适当取 $\alpha-\delta\beta$ 中的 δ 使 $\sigma(\alpha-\delta\beta)<\sigma(\beta)$. 但

$$\sigma(\alpha-\delta\beta)=\sigma\left(\beta\cdot\left(\frac{\alpha}{\beta}-\delta\right)\right)=\sigma(\beta)\sigma\left(\frac{\alpha}{\beta}-\delta\right),$$

因此取适合 $\sigma\left(\frac{\alpha}{\beta}-\delta\right)<1$ 的 δ 即可. 因为

$$\frac{\alpha}{\beta}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i,$$

如果 $\delta=u+vi$，那么

$$\frac{\alpha}{\beta}-\delta=\left(\frac{ac+bd}{a^2+d^2}-u\right)+\left(\frac{bc-ad}{c^2+d^2}-v\right)i.$$

取适合

$$\left|\frac{ac+bd}{c^2+d^2}-u\right|\leqslant\frac{1}{2},\ \left|\frac{bc-ad}{c^2+d^2}-v\right|\leqslant\frac{1}{2}$$

的整数 u,v 即得 $\sigma\left(\frac{\alpha}{\beta}-\delta\right)\leqslant\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$.

6. 假定 $f(x)=\Sigma a_ix^i$，$g(x)=\Sigma b_jx^j$，$f(x)g(x)=\Sigma c_\lambda x^\lambda$，$c_\lambda=\sum\limits_{i+j=\lambda}a_ib_j$ 因为 a_i 没有公因数，b_j 也没有公因数，命 a_i 中第一个不能用质数 p 整除的是 a_k，b_j 中第一个不能用 p 整除的是 b_l，于是 c_{k+l} 就不能用 p 整除，所以 c_λ 没有公因数.

习 题 3.10

1. 在 R 中只有一个零点 $\bar{1}$.

习 题 4.2

2. 因为环的中心是环，所以 F 的代数的中心 Z 是环，再假如 $u\in Z$，$a\in$

F,显然 $au\in Z$.

4. 因为 R 是单环,所以它的中心 Z 是域,于是对于 R 中任意正则元 a,我们有

$$a^n+c_1a^{n-1}+\cdots+c_{n-1}a+c_n=0, c_i\in Z$$

因为 a 不是零因子,所以我们可以假定 $c_n\neq 0$,因此

$$(a^{n-1}+c_1a^{n-2}+\cdots+c_{n-1})a+c_n=0,$$

即
$$\{-c_n^{-1}(a^{n-1}+c_1a^{n-2}+\cdots+c_{n-1})\}a=e,$$

所以 a 是可逆元.

5. 设 $uu=ru$,如果 $r=0$,那么 $(au)(bu)=abuu=0$,这时 Fu 是零代数,当然是结合代数,如果 $r\neq 0$,那么

$$u(uu)=u\cdot ru=ru^2=r^2u, (uu)u=ru\cdot u=r^2u$$

所以 $u(uu)=(uu)u$. 因此 Fu 是结合代数,这时 $e=r^{-1}u$ 是它的单位元.

习　题　5.2

1. 因为质域是所有子体的交集,所以它在中心里面.

2. $2=(1-i)(1+i)=0(1+i)$,所以特征数是 2.

4. 假定 P 是 K 的质域,因为 x^p-x 在 K 中的零点不多于 p 个,而 P 中 p 个元都是它的零点,所以 $K=P$.

5. 因为 $2a=(2a)^2=4a^2=4a$,所以 $2a=0$. 又因为 $a+b=(a+b)=a^2+ab+ba+b^2=a+ab+ba+b$,所以 $ab+ba=0$,于是 $ab+2ba=ba$,即 $ab=ba$.

6. 设 a 为 K 中任意元,取 $x\in K$,由 $(a+x)^p=a^p+x^p$,得

$$pa^{p-1}x+\frac{p(p-1)}{2!}a^{p-2}x^2+\cdots+pax^{p-1}=0.$$

如果 $pa\neq 0$,上式就是 x 的 $p-1$ 次多项式,它在 K 中最多有 $p-1$ 个互异的零,这显然是矛盾.

习　题　5.3

1. $$\frac{1-7\alpha+2\alpha^2}{1+\alpha-\alpha^2}=\frac{3\alpha-13}{-4(\alpha-2)}=\frac{(3\alpha-13)(\alpha-3)}{-4(\alpha-2)(\alpha-3)}$$
$$=\frac{1}{4}(-7\alpha+18).$$

2. $-1+\sqrt[3]{2}$.

3. 因为 i 适合既约多项式 x^2+1，所以 $F(i)\simeq F[x]-(x^2+1)$.

4. 因为 $\alpha=\dfrac{-1+\sqrt{3}\,i}{2}$，所以 $F(\alpha)=F(i)$，即 $F(\alpha)$是复数域.

5. $K(\alpha)=K(x^{\frac{1}{p}})=F(x^{\frac{1}{p}})=F(\alpha)$，$z^p-x=(z-\alpha)^p$.

6. 因为 $F[x]\sim F[\alpha]$，$f(\alpha)=0$，所以 $f(x)\equiv 0(p(x))$.

7. 因为$\dfrac{1}{\alpha}\in F[\alpha]$，所以$\dfrac{1}{\alpha}=f(\alpha)$，即 $\alpha f(\alpha)=1$.

习 题 5.4

1. 假如 S 是体，$0\neq a\in R$，$a^n+c_1a^{n-1}+\cdots+c_n=0$，$c_i\in S$，因为 R 是无零因子环，可以假定 $c_n\neq 0$，于是

$$\{-c_n^{-1}(a^{n-1}+c_1a^{n-2}+\cdots+c_{n-1})\}a=e$$

所以 $a^{-1}\in R$，因此 R 成体. 再假如 R 是体，$0\neq b\in S$，$b^{-1}\in R$，于是$(b^{-1})^m+d_1(b^{-1})^{m-1}+\cdots+d_m=0$，$d_i\in S$，即

$$b^{-1}=-(d_1+d_2b+\cdots+d_mb^{m-1})\in S$$

所以 S 成体.

2. 假如$\sqrt{b}=m+n\sqrt{a}$，那么 $b=m^2+n^2a+2mn\sqrt{a}$，首先 $mn^2=0$，因为不如此，b 不是整数. 再 $n\neq 0$，因为不如此，b 有相同的质因数. 于是 $m=0$，因此 $b=n^2a$. 假定 $n=\dfrac{r}{s}$，那么 $s^2b=r^2a$. 于是 $r^2|b$，$s^2|a$，所以 $r=\pm 1$，$s=\pm 1$，因此 $b=a$.

习 题 5.5

1. 因为 $x^3-x^2-x-2=(x-2)(x^2+x+1)$，所以分裂域是 $Q(\sqrt{-3})$.

2. 因为 $x^4+4x^2+2=(x^2+2-\sqrt{2})(x^2+2+\sqrt{2})$，所以它的零点是 $\pm\sqrt{2-\sqrt{2}}\,i$，$\pm\sqrt{2+\sqrt{2}}\,i$. 又因为$\sqrt{2}\in K=Q(\sqrt{2-\sqrt{2}}\,i)$，所以

$$\sqrt{2+\sqrt{2}}\,i=-\frac{\sqrt{2}}{\sqrt{2-\sqrt{2}}\,i}\in K.$$

3. 因为$(F(\alpha):F)=2$，所以 α 满足的既约多项式 $f(x)$的次数是 2，因此 $F(\alpha)$是 $f(x)$的分裂域.

5. 因为 K 中任意元是在添加有穷个多项式的零点于 F 的域中.

6. 因为 3 次多项式 $f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$的判别式

$$D=\{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\}^2>0$$

时，$\alpha_1,\alpha_2,\alpha_3$是 3 个不同的实根，又因为

$$(x-\alpha_2)(x-\alpha_3)=x^2-(\alpha_2+\alpha_3)x+\alpha_2\alpha_3\in Q(\alpha_1)[x],$$

所以
$$\alpha_2+\alpha_3,\alpha_2\alpha_3,(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\in Q(\alpha_1).$$

假如$\sqrt{D}\in Q$，那么 $\alpha_2-\alpha_3=\sqrt{D}/(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\in Q(\alpha_1)$，因此 α_2，$\alpha_3\in Z(\alpha_1)$，所以 $f(x)$是 Q 的正规式.

假如 $\alpha_2,\alpha_3\in Q(\alpha_1)$，那么$\sqrt{D}=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)=a\in Q(\alpha_1)$，如果 $a\overline{\in}Q$，那么$(Q(a):Q)=2$，这与$(Q(\alpha_1):Q)=3$ 的性质矛盾. 所以 $a\in Q$，即 D 是有理数的平方.

习 题 5.6

1. 因为 $x^{\frac{1}{p}}\overline{\in}F(x)$，所以 $y^p-x=(y-x^{\frac{1}{p}})^p$ 在 $F(x)[y]$中是既约的.

3. 两个可离元的乘积是可离元，一个可离元与一个不可离元的乘积是不可离元，两个不可离元的乘积或是可离元或是不可离元.

4. 假如 F 是完全域，因为 $x^p-a=(x-a^{\frac{1}{p}})^p$ 有重零点，所以它在 $F[x]$中不是既约的. 于是 $x-a^{\frac{1}{p}}\in F[x]$，即 $a^{\frac{1}{p}}\in F$. 反过来，假如 F 中任意元的 p 乘根都在 F 中，因为 x^p 的任意多项式

$$f(x)=\Sigma a_i x^{ip}=(\Sigma a_i^{\frac{1}{p}} x^i)^p$$

都不是既约的，所以 $F[x]$中的既约多项式都是可离多项式.

5. 假如 K 是完全域 F 的代数域，K 的代数元 α 适合既约多项式 $f(x)=\Sigma a_i x^i$，显然 α^p 是既约多项式 $g(x)=\Sigma a_i^p x^i$ 的零点，于是 $F(\alpha)=F(\alpha^p)$. 所以 $\alpha=\Sigma b_i\alpha^{ip}=(\Sigma b_i^{\frac{1}{p}}\alpha^i)^p$，即 $\alpha^{\frac{1}{p}}\in F(\alpha)$，因此 K 是完全域.

再假如 K 是不完全域 F 的 n 次扩张域，$u_1,\cdots,u_n$ 是 K 关于 F 的底，显然 $u_1^p,\cdots,u_n^p$ 是 K^p 关于 K^p 的底. 于是$(K:F)=(K^p:F^p)$. 如果 $K=K^p$，那么 $F=F^p$，这与 F 是不完全域的假设不合. 因此 $K\supset K^p$. 所以 K 是不完全域.

6. 假定 K 中元 α 的指数是 k，因为 $x^{p^k}-\alpha^{p^k}=(x-\alpha)^{p^k}$在 $F[x]$中是既约的，所以 K 是 F 的正规域. 又假定 $\alpha\to\alpha'$是 K 关于 F 的同值映射，因为 $\alpha^{p^k}\in F$，所以 $\alpha'^{p^k}\in F$，于是 $\alpha^{p^k}=\alpha'^{p^k}$，因此 $\alpha=\alpha'$. 所以 K 关于 F 的同值映射是恒等映射.

7. 因为 K 关于 F 的同值映射可以看成 L 关于 F 的同值映射的延长，而

K 是 L 的纯不可离域，纯不可离域的同值映射只是不动映射，所以 K 关于 F 的同值映射只有$(L:F)$个.

8. 因为 K 关于 F 的缩减次数是 K 关于 F 的互异同值映射的个数.

10. 假定 β 是 $F(\alpha)$中关于 F 的可离元，那么 $F(\beta)$有$(F(\beta):F)$个关于 F 的同值映射，把这些映射延长就得到 $F(\alpha)$关于 F 的同值映射. 但这时$F(\alpha)$关于 F 的同值映射，显然只有 1 个恒等映射. 因此 $F(\beta)=F$，即 $\beta\in F$. 所以 $F(\alpha)$是 F 的纯不可离域. 再假如 α_1,α_2 是 F 的纯不可离元，于是 $F(\alpha_1,\alpha_2)$是 $F(\alpha_1)$的纯不可离域，由传递律得知 $F(\alpha_1,\alpha_2)$也是 F 的纯不可离域.

习 题 5.7

1. $\sqrt{3}+\sqrt[3]{2}$.

2. $\sqrt{2}+i$

3. $(F(x^{\frac{1}{p}},y^{\frac{1}{p}}):F(x,y))=p^2$，即 $n=p^2$，但这时 $k=1$.

习 题 5.8

1. 因为 $Z-(p)$是元数为 p 的有穷域，所以对于任意 $a\not\equiv 0(p)$，有 $a^{p-1}\equiv 1(p)$.

2. 因为 $f(x)=\sum_{i=0}^{m}a_ix^i$，$a_i^p=a_i$，所以 $f(\alpha^p)=\sum a_i^p\alpha^{ip}=(\sum a_i\alpha^i)^p=0$，即 α^p 是 $f(x)$的零点. 同样 $\alpha^{p^2},\cdots,\alpha^{p^m}$都是 $f(x)$的零点. 因为$(F(\alpha):F)=m$，所以 $F(\alpha)=GF(p^m)$，因此 $\alpha^{p^m}=\alpha$.

3. 假定 $\alpha\in GF(p^n)$，那么 $\alpha^{p^n}=\alpha$，即$(\alpha^{p^{n-1}})^p=\alpha$，所以 $\alpha^{p^{n-1}}$是 α 的 p 次幂. 于是由§5.6 习题 4 即得.

4. 假如 $a^{\frac{1}{p}}=x$，$a^{\frac{1}{p}}=y$，那么 $a=x^p=y^p$，于是$(x-y)^p=0$，所以 $x=y$.

5. 设 F 的特征数为 p，因此 K 的元数为 p^n.

$$L_\alpha=\{1+\alpha x^2\mid x\in K\}$$

当 $1+\alpha x^2=1+\alpha y^2$ 时，$x^2=y^2$，所以 $x=\pm y$，即对于 x 及 $-x$，L_α 中只有一元. 又因为 $x=0$ 时，$1\in L_\alpha$，于是 L_α 共有 $1+\frac{p^n-1}{2}=\frac{p^n+1}{2}$个元. 同样，$L_\beta=\{-\beta x^2\mid x\in K\}$也有$\frac{p^n+1}{2}$个元，两者都过$|K|$的半数，因此 $L_\alpha\cap L_\beta\neq 0$. 于是有 $c=1+\alpha x^2$，$c=-\beta y^2$，所以 $1+\alpha x^2+\beta y^2=0$.

6. 因为 h 次单位根得由 h 次本原单位根的乘幂而成.

7. 假定 F 是 $K=GF(3^2)$ 的质域，因为 K 是 $f(x)=x^9-x=(x^4+1)(x^2+1)(x^2-1)x$ 的分裂域，因为 $x^4+1=(x^2-1)^2-x^2=(x^2+x-1)(x^2-x-1)$，又 $x^2+x-1=(x-1)^2-2=(x-1)^2+1=0$ 时，$x=1\pm i$，这里 i 是 $x^2+1=0$ 的零点，同样 $x^2-x-1=0$ 时，$x=-1\pm i$ 所以 $K=\{0,\pm1,\pm i,\pm1\pm i\}$. 因为 $1+i$ 是 K 中阶是 8 的元，所以 K 的乘群 $K^*=(1+i)$.

习 题 5.9

1. 假定 $u_1,\cdots,u_m$ 是 K 关于 L 的代数底，$v_1,\cdots,v_n$ 是 L 关于 F 的代数底，那么 $M=\{u_1,\cdots,u_m,v_1,\cdots,v_n\}$ 关于 F 代数无关，这是因为如果 u_1 与 $M-u_1$ 或 v_1 与 $M-v_1$ 关于 F 代数相关，显然 $\{u_1,\cdots,u_m\}$ 关于 L 代数相关，这与假设不合. 再因为 $\{u_1,\cdots,u_m\}$ 是 K 关于 L 的代数底，所以 K 是 $L(u_1,\cdots,u_m)$ 的代数域. 又因为 L 是 $F(v_1,\cdots,v_n)$ 的代数域，所以 $L(u_1,\cdots,u_m)$ 是 $F(M)$ 的代数域，因此 K 是 $F(M)$ 的代数域. 于是 K 中任意元关于 F 与 M 代数相关. 所以 M 是 K 关于 F 的代数底.

2. 因为 $F(u,v)\supset F(u,v^2+u)\supset F(u^3+v^2,v^2+u)$.

3. $F(x)$ 关于 F 的任一自同值是把 x 变为 $F(x)$ 的本原元 $u=\dfrac{ax+b}{cx+d}$，$ad-bc\neq0$.

习 题 6.1

1. 因为同态把子群 H 变为子群 H'. 假如 $h'\in H'$. 由 $h\to h'$ 有 $\lambda h\to\lambda h'$，但 $\lambda h\in H$，所以 $\lambda h'\in H'$，因此 H' 是带算子群.

2. 假如 $G=(a)$，$\lambda a=a^k$，$H=(a^m)$，那么 $\lambda a^m=(\lambda a)^m=(a^m)^k\in H$.

3. 假定 λ 是算子，因为正规子群的同态象仍然是正规子群，所以 λA_4，λB_4 都是正规子群，因为 S_4 的正规子群只有 A_4，B_4，所以 $\lambda A_4\subseteq A_4$，$\lambda B_4\subseteq B_4$，所以 A_4，B_4 都是带算子群.

4. 假定 λ 是算子，因为

$$\lambda(a^{-1}b^{-1}ab)=(\lambda a)^{-1}(\lambda b)^{-1}(\lambda a)(\lambda b)\in D(G)$$

所以由换位子生成的子群是带算子群，即 $D(G)$ 是带算子群.

5. 因为 $(a,0)\to(0,a)$ 时 $(a,0)(b,0)$ 与 $(0,a)(0,b)$ 对应，但 $(\lambda_1,\lambda_2)(a,0)=(\lambda_1a,0)$，$(\lambda_1,\lambda_2)(0,a)=(0,\lambda_2a)$，所以 $(\lambda_1,\lambda_2)(a,0)$ 不与 $(\lambda_1,\lambda_2)(0,a)$ 对应.

习 题 6.2

1. 因为$S_4=S_3B_4$，而$S_3\cap B_4=(1)$，所以$S_4/B_4\simeq S_3$.

2. 因为$S_n=G\cdot A_n$，所以$S_n/A_n=G\cdot A_n/A_n\simeq G/G\cap A_n=G/H$.

3. 由第三同构定理，$H\cap K/H\cap K'\simeq K'(K\cap H)/K'\subseteq K/K'$.

5. $F(a)\simeq\{Z-(p)\}[x]-A$，因为$Z\sim Z-(p)$，所以$Z[x]\sim\{Z-(p)\}[x]$，假如A在$Z[x]$的完全象源是N，那么$\{Z-(p)\}[x]-A\simeq Z[x]-N$，因此$F(a)\simeq Z[x]-N$.

习 题 6.3

1. S_2是交换群，$S_3\supset A_3\supset 1$的商群列的元数是2，3，所以都是可解群.

2. 因为$G/H=\overline{G}_0$，H都是可解群，所以它们有商群是交换群的正规群列$\overline{G}_0\supset\overline{G}_1\supset\cdots\supset\overline{G}_m=E$，$H=H_0\supset H_1\supset\cdots\supset H_n=E$. 命$G_i$是$\overline{G}_i$在$G$中的完全象源，那么$G=G_0\supset G_1\supset\cdots\supset G_m=H=H_0\supset H_1\supset\cdots\supset H_n=E$.

3. 由第二同构定理，HK/K是可解群，又因为K是可解群，所以HK是可解群.

5. S_4的所有合成群列为$S_4\supset A_4\supset B_4\supset C_i\supset E$，这里

$$C_1=\{(1),(12)(34)\},C_2=\{(1),(13)(24)\},$$
$$C_3=\{(1),(14)(23)\}.$$

6. 无穷交换群的极大子群仍然是无穷群.

9. 因为G/N是幂零群，所以$(G/N)^{(n)}=E$，即$G^{(n)}\subseteq N$但$N\subseteq Z(G)$，所以$N^{(1)}=E$，于是$G^{(n+1)}=E$，所以G是幂零群.

10. 因为$Q(\sqrt[4]{2},i)\supset Q(\sqrt[4]{2})\supset Q(\sqrt{2})\supset Q$是$Q(\sqrt[4]{2},i)$的合成体列.

习 题 6.4

1. 由$ur+us=1$得$a=(a^r)^u\cdot(a^s)^v$，因此$(a)=(a^r)\cdot(a^s)$. 再命$b\in(a^r)\cap(a^s)$，那么$b=a^{sh}=a^{rk}$，于是$sh\equiv rk(n)$，即$sh-rk=mn=mrs$，因此$sh=r(k+ms)$，所以$r|h$，因此$b=c$，即$(a^r)\cap(a^s)=e$.

3. 假如$A=\{e,a,a^2\}$，$B=\{c,b,b^2\}$，那么

$$A\times B=\{e,a,a^2,b,ab,a^2b,b^2,ab^2,a^2b^2\}.$$

5. 假设 $G/H=(\bar{a})$，$K=(e)$，显然 $K\simeq G/H$，并且 $G=HK$.

6. 因为 $G=AB$，所以 $g=ab$，于是 $\bar{g}=\overline{ab}$，因此 $\overline{G}=\overline{A}\ \overline{B}$. 再 $\overline{A}$，$\overline{B}$ 都是 $\overline{G}$ 的正规子群，假如 $\bar{c}\in\overline{A}\cap\overline{B}$，那么 $c\in A\cap B=H$，因此 $\bar{c}=\bar{e}$，即 $\overline{A}\cap\overline{B}=\bar{e}$.

7. 因为 $A\times B$ 的长 $=A$ 的长 $+B$ 的长，$\overline{G}=G/H$ 时，G 的长 $=\overline{G}$ 的长 $+$ H 的长.

8. 假定 $c\in Z$，$c=a_1+\cdots+a_n$，$a_i\in R_i$，对于 R_i 中任一元 r_i，因为 $R_iR_j=0$，$i\neq j$，所以 $cr_i=a_1r_i+\cdots+a_nr_i=a_ir_i$，于是 $a_i\in Z_i$，因此 Z 是 $Z_1,\cdots,Z_n$ 的和，再因为 R 是 $R_1,\cdots,R_n$ 的直和，所以 $c=a_1+\cdots+a_n$ 的表示是唯一的.

10. 因为 $ee_j=e_j=e_1e_j+\cdots+e_je_j+\cdots+e_ne_j=\sum\limits_{i=1}^{n}e_ie_j$，所以 $e_ie_j=0$，$i\neq j$，$ee_i=e_i=e_i^2$. 反过来，假如 $e=e_1+\cdots+e_n$，$e_ie_j=0$，$i\neq j$，$e_i^2=e_i$，那么 $r=re=re_1+\cdots+re_n$，即 R 是 $L_1=Re_1,\cdots,L_n=Re_n$ 的和. 再当 $r_1e_1+\cdots+r_ne_n=0$，两边用 e_i 右乘即得 $r_ie_i=0$，所以这表示又是唯一的. 因此 R 是 $L_1,\cdots,L_n$ 的直和.

11. 假定 e 是 R 的幂等元，但不是单位元，那么 R 中所有满足 $r_1e=er_1=r_1$ 的元 r_1 形成理想 R_1，显然 e_1 是 R_1 的单位元.

习 题 6.5

1. 循环群与非循环群两类，前者是 2 元群与 9 元循环群的直积，后者是 2 元群与两个 3 元群的直积.

2. 设 G 是 6 元群，如果它有阶数为 6 的元，那么 G 是循环群，如果没有阶数为 6 的元，那么 G 有阶数为 3 的元，因为阶数都是 2 时 G 是交换群，这时 G 是 2 元群与 3 元群的直积，这显然不对，假定 a，a^2，$a^3=1$，b 是 G 中另一元，容易验证 $1,a,a^2,b,ab,a^2b$ 互异，于是 $G=\{1,a,a^2,b,ab,a^2b\}$. 再 b^2 只能是 1，即 $b^2=1$，又可能 $ba=ab$ 或 $ba=a^2b$，如果 $ba=ab$，那么 $(ab)^6=1$，此不可. 因此 $ba=a^2b$，即 $(ab)^2=1$. 这就是说 $a^3=b^2=(ab)^2=1$，这是 S_3 的结构，所以 $G\simeq S_3$.

3. 假定 $G=(a)$ 的元数 $n=pq$，$(p,q)=1$. 因为 G 中任意元的阶都是 n 的约数，所以 n 是它们的公倍数. 但 a^p 的阶是 q，a^q 的阶是 p，所以 n 是它们的最小公倍. 反过来，由 § 2.2 习题 4，G 中有阶为 n 的元，因此 G 是循环群.

4. 周期群不一定是有穷群. 譬如 $0\leqslant x<1$ 的有理数 x 的集合 G，其中任意两元的加法与普通的一样，只是当其和不小于 1 时，要减少 1，譬如 $\frac{1}{2}+\frac{2}{3}$

$=\frac{1}{6}$，$\frac{1}{2}+\frac{1}{2}=0$，显然 G 对这加法成为群，其中任意元的阶数都是有穷，譬如 $3\cdot\frac{2}{3}=0$，即$\frac{2}{3}$的阶数是 3，所以 G 是周期群.

5. 假定$G=(a_1)\times(a_2)\times(a_3)\times(a_4)\times(a_5)$，它们的元数分别是 $2^3,2^4,3,3^2,3^4$. 命 $G_1=(a_3)$，$G_2=(a_1)\times(a_4)=(a_1a_4)$，$G_3=(a_2)\times(a_5)=(a_2a_5)$，显然 $G=G_1\times G_2\times G_3$，这时 G_1,G_2,G_3 的元数分别是 $3,2^3\cdot3^2,2^4\cdot3^3$.

6. 因为 $\chi_0(a)=e$，所以$\sum_{i=1}^{n}\chi_0(a_i)=ne$. 又因为 $\chi(a_i)=\xi_i$，所以$\sum_{i=1}^{n}\chi(a_i)=\sum_{i=1}^{n}\xi_i$. 但 ξ_i 是 $x^{n_i}=e$ 的零点，因此也是 $x^n=e$ 的零点，所以$\sum_{i=1}^{n}\xi_i=0$.

习　题　6.6

1. 把 G 就 G_a 分为陪集 τ_iG_a，因为 G 是可迁群，所以这样的陪集有 m 个，如果 G_a 的元数是 q，那么 G 的元数 $n=mp$.

2. 因为 $G_{\tau(a)}=\tau G_a\tau^{-1}$，所以 G_a 与 $G_{\tau(a)}$ 共轭. 假如 G_a 中任意变换不使文字 b 变动，那么 $G_a\subseteq G_b$，但 G_a,G_b 的元数相等，因此 $G_a=G_b$，于是 $G_a=\tau G_a\tau^{-1}$，即 τ 与 G_a 能够交换.

4. 所求的二个非原系为{1,4}，{2,5}，{3,6}及{1,3,5}，{2,4,6}.

5. H 的所有非原系为{1,2}，{3,4}，{5,6}；{1,3}，{2,5}，{4,6}；{1,6}，{2,4}，{3,5}及{1,4,5}，{2,3,6}.

习　题　7.1

1. 假定 $f(x)$ 是 $F[x]$ 中的 3 次既约多项式，如果 $f(x)$ 是正规式，那么 $(K:F)=3$，因此 $G=A_3$. 如果 $f(x)$ 不是正规式，那么 $(K:F)=6$. 因此 $G=S_3$.

2. 因为$\sqrt{D}=\prod_{1\leqslant i<j\leqslant n}(a_i-a_j)=d$，由 § 2.2 定理 3 的证明得知偶排列不使 d 变动，奇排列把 d 变为 $-d$. 于是假如 G 是全由偶排列所成，那么 $d\in F$ 即 D 的平方根在 F 中. 反过来，假如 $d\in F$ 那么 G 中任意元不使 d 变动，因此 G 是全由偶排列组成的.

3.

	1	σ	τ	ρ
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
i	i	$-i$	i	$-i$

	1	σ	τ	ρ
1	1	σ	τ	ρ
σ	σ	1	ρ	τ
τ	τ	ρ	1	σ
ρ	ρ	τ	σ	1

5. 由§5.5习题6，x^3-2，x^3+2x+1都不是正规式，因此它们的伽罗瓦群都是S_3. 又因为

$$x^4-10x^2+1=(x^2-1)^2-8x^2=\{(x-\sqrt{2})^2-3\}\{(x+\sqrt{2})^2-3\}$$
$$=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}),$$

所以其分裂域$K=Q(\sqrt{2},\sqrt{3})$. 于是其伽罗瓦群$G=\{1,\sigma,\tau,\rho\}$的群表为

	1	2	3	4
1	1	2	3	4
σ	2	1	4	3
τ	3	4	1	2
ρ	4	3	2	1

其中$1=\sqrt{2}+\sqrt{3}$，$2=\sqrt{2}-\sqrt{3}$，
$3=-\sqrt{2}+\sqrt{3}$，$4=-\sqrt{2}-\sqrt{3}$.

6. 因为在$Q[x]$中x^4-10^2+1是既约的，而x^4-5x^2+6是可约的，所以前者的伽罗瓦群是可迁群而后者的是非迁群. 又因为

$$x^4-5x^2+6=(x^2-2)(x^2-3)$$
$$=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3}),$$

它的伽罗瓦群$G=\{1,\sigma,\tau,\rho\}$的群表为

	1	2	3	4
1	1	2	3	4
σ	2	1	3	4
τ	1	2	4	3
ρ	2	1	4	3

其中$1=\sqrt{2}$,$2=-\sqrt{2}$,

$3=\sqrt{3}$,$4=-\sqrt{3}$.

7. 由定理 2,$K=F(\alpha)$,α 是多项式 x^p-a 的零点,的伽罗瓦群与 p 次单位根形成的 p 元循环群的子群同构,但 p 元循环群的子群只有自身及单位元群. 从前者言,x^p-a 在 $F[x]$中是既约的,从后者言,x^p-a 在 $F[x]$中完全分裂.

8. 假如 $x^p-a=f(x)g(x)=\pi(x-\varepsilon^i\alpha)$,$\alpha^p=a$,那么 $f(x)$中不含 x 的项 $\pm b$ 必为$\pm\varepsilon^l\alpha^k$,即 $b=\varepsilon^l\alpha^k$. 于是 $b^p=\alpha^{p^k}=a^k$,$0<k<p$. 因此$(k,p)=1$,即 $rk+sp=1$. 所以

$$a=a^{rk}\cdot a^{sp}=b^{rp}\cdot a^{sp}=(b^r a^s)^p=\alpha^p,\alpha=b^r a^s\in F,$$

于是
$$x^p-a=x^p-\alpha^p=(x-\alpha)(x^{p-1}+\alpha x^{p-2}+\cdots+\alpha^{p-1}).$$

习　题　7.2

1. 假定(G_1,G_2)所属的域是 K',因为 $G_i\subseteq(G_1,G_2)$,所以 $K'\subseteq K(G_i)$,因此 $K'\subseteq K(G_1)\cap K(G_2)$. 再命 $\alpha\in K(G_1)\cap K(G_2)$,那么 G_1,G_2 中任意元不使 α 变动,因此(G_1,G_2)中任意元也不使 α 变动. 于是 $\alpha\in K'$,即 $K(G_1)\cap K(G_2)\subseteq K'$. 因此 $K'=K(G_1)\cap K(G_2)$.

又假定 $G_1\cap G_2$ 所属的体是 K'',因为 $G_1\cap G_2\subseteq G_i$,所以 $K(G_1)$,$K(G_2)\subseteq K''$. 于是 $F(K(G_1),K(G_2))\subseteq K''$. 但 $F(K(G_1),K(G_2))$所属的群 G' 显然是 $G_1\cap G_2$ 的子群,即 $G'\subseteq G_1\cap G_2$,所以 $F(K(G_1),K(G_2))\supseteq K''$. 因此 $K''=F(K(G_1),K(G_2))$.

2. 因为 $F(K_1,K_2)$所属的群 $G'\subseteq G(K_1)\cap G(K_2)$. 但 $G(K_1)\cap G(K_2)$所属的域是 $F(K_1,K_2)$,因此 $G'=G(K_1)\cap G(K_2)$.

又因为 $K_1\cap K_2$ 所属的群 $G''\supseteq G(K_i)$,所以 $G''\supseteq(G(K_1),G(K_2))$. 但$(G(K_1),G(K_2))$所属的域是 $K_1\cap K_2$,因此 $G''=(G(K_1),G(K_2))$.

3. 因为 $F(\alpha)$是 F 的正规域,所以 $K(\alpha)$也是 K 的正规域. 假如 $K(\alpha)$关于 K 的伽罗瓦群 G 与 $F(\alpha)$关于 F 的伽罗瓦群 G' 一致,因为 G 中任意元不

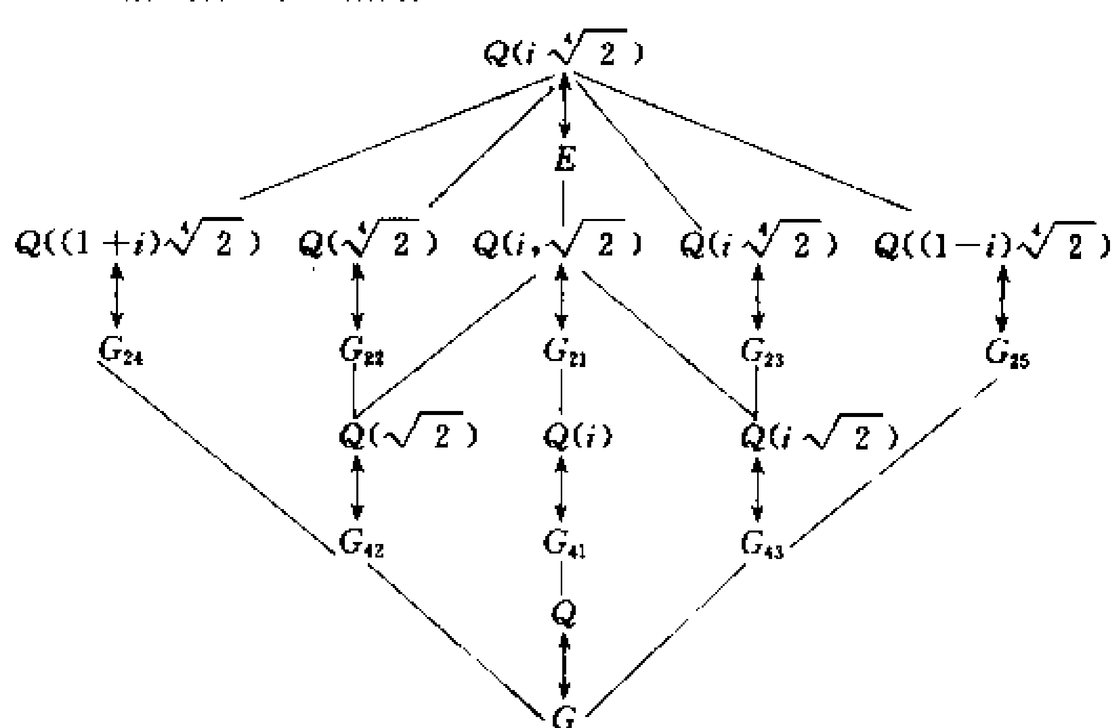
使 K 中任意元变动，当然也不使 F 中任意元变动，并且 $F(\alpha)$ 中元对于 G 中任意不变动的只有 F 中元，因此 $F(\alpha)\cap K=F$.

反过来，假如 $F(\alpha)\cap K=F$，那么 $F[x]$ 中 α 适合的既约多项式 $f(x)$ 也是 $K[x]$ 中 α 适合的既约多项式. 因此 $f(x)$ 在 $F(\alpha)$ 中的零点 $\alpha=\alpha_1,\cdots,\alpha_n$ 也是 $f(x)$ 在 $F(\alpha)$ 中的零点. 于是 $\alpha\to\alpha_i$ 是 G' 中元也是 G 中元，所以 G 与 G' 一致.

4. 假定 $K\supseteq K_1\supseteq F$，$G(K_1)=G_1$，因为 G 是阿贝耳群，所以 G 的子群 $G_1\lhd G$，因此 K_1 是 F 的正规域.

5. 假定 L_i 是 K 中 L 的共轭子域，那么 $F(L,L_1,\cdots)$ 是 K 中包含 L 的 F 的最小正规域，于是 $F'=F(L,L_1,\cdots)$，因此它的伽罗瓦解 $G'=G(K)\cap G(L_1)\cap\cdots$.

6. 请先看图式后的解答.



解答：K 的伽罗瓦群 G 是 8 元群，其元素为

	1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

再因为 K,Q 的中间体中，关于 Q 是 2 次的有 3 个：

$$Q(i),Q(\sqrt{2}),Q(i\sqrt{2}),$$

它们所属的群都是 4 元群，分别为

$$G_{41}=\{1,\sigma,\sigma^2,\sigma^3\},G_{42}=\{1,\sigma^2,\tau,\sigma^2\tau\},G_{43}=\{1,\sigma^3,\sigma\tau,\sigma^3\tau\};$$

关于 Q 是 4 次的 有 5 个：

$Q(i,\sqrt{2}),Q(\sqrt[4]{2}),Q(i\sqrt[4]{2}),Q((1+i)\sqrt[4]{2}),Q((1-i)\sqrt[4]{2})$,

它们所属的群都是 2 元群，分别为

$$G_{21}=\{1,\sigma^2\},G_{22}=\{1,\tau\},G_{23}=\{1,\sigma^2\tau\}$$
$$G_{24}=\{1,\sigma\tau\},G_{25}=\{1,\sigma^3\tau\}.$$

它们之间的关系如上页图式所示.

7. 1)是显然的.

2)因为 G 中任意元把 K 中 F 的可离元仍然变为可离元，所以它把 L 仍然变为 L，并且它不使 F 中任意元变动. 又 G 的元数是 n_0，而 $(L:F)=n_0$，所以 G 可以看成 L 关于 F 的伽罗瓦群.

3)显然 G 中不使 K_1 中任意元变动的元也不使 L_1 中任意元变动，反过来，假如 σ 不使 L_1 中任意元变动，$\alpha\in K_1$，$\alpha^{p}\in L_1$，由 $\sigma\alpha^{p^k}=\alpha^{p^k}$ 即得 $(\sigma\alpha-\alpha)^{p^k}=0$，于是 $\sigma\alpha=\alpha$. 所以 σ 也不使 K_1 中任意元变动.

4)假如 $\alpha^p=a\in K_1$，$\alpha_1^p=a$，因为 $(\alpha-\alpha_1)^p=0$，所以 $\alpha=\alpha_1$，这就是说 $x^p=a$ 只有一个 p 重根. 因为 G_1 中任意元把 $x^p=a$ 的零点仍然变为它的零点，因此它不使 α 变动，所以 $\alpha\in K_1$.

5)因为 G 中不使 $L(G_1)$ 中任意元变动的元，同样也不使 $K(G)$ 中任意元变动，所以 $G(K(G_1))$ 的元数等于 $G(L(G_1))$ 的元数，但 G 也可以看成 L 关于 F 的伽罗瓦群，并且

$$G(L(G_1))=G_1,G(K(G_1))\supseteq G_1$$

所以 $G(K(G_1))=G_1$.

6)假定 $\alpha\in K(G(K_1))$，$\alpha^{p^k}\in L(G(K_1))$，因为 $G(K_1)=G(L_1)$，并且 $L(G(K_1))=L(G(L_1))=L_1$ 所以 $\alpha^{p^k}\in L_1$，因此 $\alpha\in K_1$.

习 题 7.5

1. 因为 $n\geqslant5$ 时. A_n 是单群，所以 $S_n\supset A_n\supset E$ 是 S_n 的合成群列，但 A_n 是非交换群.

3. x^5-4x+2 有三个实根，所以它不能用根号解出.

习 题 8.1

2. 假定 $V=V_1+\cdots+V_n$，如果对 V 中任意 $n+1$ 个非零元 $\alpha_1,\cdots\alpha_{n+1}$ 我们

有 $\alpha_{n+1}=a_1\alpha_1+\cdots+a_n\alpha_n, a_i\in R$，那么 n 是由 V 唯一确定，下面我们对 n 用归纳法来证明.

当 $n=1$ 时，$V=V_1$，即 V 是既约的，因为 $\alpha_1\neq 0, R\alpha_1\neq 0$，那么 $R\alpha_1=V_1$ 即 $R\alpha_1=V$. 所以 $\alpha_2=a_2\alpha_1$. 假定 $n-1$ 时，性质成立. 设 $\alpha_i=\alpha_{i1}+\cdots+\alpha_{in}, \alpha_{ij}\in V_j$. 我们可以假定 $\alpha_{11}\neq 0$，由 $R\alpha_{11}=V_1$，得 $\alpha_{i1}=a_i\alpha_{11}$. 于是

$$\alpha_i'=\alpha_i-a_i\alpha_1=(\alpha_{i2}-a_i\alpha_{i2})+\cdots+(\alpha_{in}-a_i\alpha_{1n}), i=2,\cdots,n$$

即 α'_i 是 $V'=V_2+\cdots+V_n$ 中元，根据归纳法假设，我们有 $\alpha'_{n+1}=b_2\alpha_2+\cdots+b_n\alpha'_n$，因此 $\alpha_{n+1}-a_{n+1}\alpha_1=b_2(\alpha_2-a_2\alpha_1)+\cdots+b_n(\alpha_n-a_n\alpha_1)$

所以 $$\alpha_{n+1}=(a_{n+1}-a_2-\cdots-a_n)\alpha_1+b_2\alpha_2+\cdots+b_n\alpha_n.$$

3. 因为 $Z_2\begin{pmatrix}2 & 0\\ 2 & 0\end{pmatrix}\supset Z_2\begin{pmatrix}4 & 0\\ 4 & 0\end{pmatrix}\supset\cdots$，所以 Z'_2 不满足极小条件.

习 题 8.2

1. Fu_3.

2. 因为 m 不能用质数平方整除时，$Z-(m)$ 中没有异于零的幂零元.

3. 假如 R 的中心的根基不为零，a 是其中一元，那么 R_a 是 R 中非零的幂零左理想，这与假设不合.

5. 假定 $L^n=0$，那么 $(L,LR)^n=0$.

6. 假定 $L^2\neq 0$，那么 L 中有元 a 使 $La\neq 0$，因此 $L=La$. 于是 L 中有元 e 使 $ea=a$. 所以 $e^2a=ea$，即 $(e^2-e)a=0$. 假定 $L'=\{b|b\in L, ba=0\}$，那么 L' 是 R 的左理想，并且 $L'\subseteq L$，但 $e\,\overline{\in}\,L'$，所以 $L'=0$，因此 $e^2=e$. 于是 $Le\neq 0$ 所以 $L=Le$.

7. 设 $N^k=0, \overline{R}^t=\overline{0}$，那么 $R^t\subseteq N$，于是 $R^{tk}\subseteq N^k=0$.

习 题 8.3

1. 由定理 5 及 § 3. 6 习题 10 即得.

2. 设 $e=g+h, g\neq 0, h\neq 0$，是正交幂等元，那么 $ge=g^2+gh=g, eg=g^2+hg=g$，所以 $g=eg=ge$，但 $g\neq e$. 反过来，假如 $g=eg=ge$，而 $0\neq g^2=g\neq e$，那么 g 及 $e-g$ 都是幂等元，并且其和为 e，所以 e 不是本原幂等元.

3. 假如 $L=Re$ 不是极小左理想，设 $L_1=Re_1\subset L$，由 $l=le_1+l-le_1$，得 $L=Le_1+L_2$，即 $L=L_1+L_2, e=e_1+e_2$，因为 $e_1=e_1e=e_1^2+e_1e_2$，所以 $e_1^2=e_1, e_1e_2$

$=0$. 同样 $e_2^2=e_2, e_2e_1=0$. 因此 e 不是本原幂等元.

4. 假定 $R=L_1+\cdots+L_n$，这里 L_i 是 R 的极小左理想，显然

$$0\subset L_1\subset L_1+L_2\subset\cdots\subset L_1+\cdots+L_n=R$$

是 R 的一个合成列，所以 R 满足极小条件再假如 N 是 R 的根基，那么 $N=NR=NL_1+\cdots+NL_n$ 但 $NL_i\subseteq L_i$. 如果 $NL_i=L_i$，因为 $N^m=0$，所以 $L_i=N^mL_i=0$，此不可. 因此 $NL_i=0$. 于是 $N=0$.

习 题 8.4

1. 由定理 2、§5.8 魏特邦定理及 §3.1 习题 8 即得.
2. 因为两个以上体的直和不再成为体.
3. 引用定理 2 及 §8.3 习题 3.

习 题 8.5

1. 因为 a 是左拟正则元，所以 $a+a'+a'a=0$，又因为 $a'=-a-a'a\in L$，所以 $a'+a''+a''a'=0$. 于是

$$\begin{aligned}a&=a+a'+a''+a''a'+(a'+a''+a''a')a\\&=a+a'+a'a+a''+a''(a'+a+a'a)=a''.\end{aligned}$$

因此 $a'a=aa'$. 再如果 $a+b+ba=0$，于是

$$\begin{aligned}b&=b+a+a'+a'a+b(a+a'+a'a)\\&=b+a+ba+a'+(a+b+ba)a'=a'.\end{aligned}$$

2. 由 $(-a^2)\circ b=0$ 得 $a\circ((-a)\circ b)=(a\circ(-a))\circ b=(-a^2)\circ b=0$.

3. 假如 $a^n\circ b=0$，n 是奇数，那么

$$a\circ\left\{\left(\sum_{i=1}^{n-1}(-a)^i\right)\circ b\right\}=\{a\circ(\sum(-a)^i)\}\circ b=0.$$

4. 假定 $ab+c+cab=0$，那么

$$ba+(-ba-bca)+(-ba-bca)ba=-b(c+ab+cab)a=0.$$

5. 因为 $\bar{R}=R-J$，所以 $(\bar{R}\,\bar{x})^2=\bar{R}\,\bar{x}\bar{R}\,\bar{x}=\bar{0}$，即 $\bar{R}\,\bar{x}$ 是 $\bar{R}$ 的幂零左理想，因此 $\bar{R}\,\bar{x}=\bar{0}$，于是 $\bar{x}^2\in\bar{R}\,\bar{x}=\bar{0}$，$(\bar{r}\,\bar{x}+\bar{n}\,\bar{x})^2\subseteq\bar{R}\,\bar{x}=\bar{0}$，即 $\bar{x}$ 生成的左理想是幂零左理想，但 $\bar{R}$ 是半单纯环，所以 $\bar{x}=\bar{0}$，因此 $x\in J$.

6. 因为 $-a\in J$，所以 $-a+a'-a'a=0$. 于是

$$0=(-a+a'-a'a)x=-ax+a'x-a'ax=-x+a'x-a'x=-x.$$

7. 由上题即得.

9. 因为$(1+a')(1+a)=1+a+a'+a'a=1$. 又因为$a'a=aa'$，所以$(1+a)(1+a')=1$.

10. 因为$r-re\in L$，显然$e\overline{\in}L$，否则$r\in L$ 即$R=L$ 这不可，于是根据冲恩引理R中有包含L而不包含a的极大左理想，这子环又是R的极大左理想，因为它是L的扩张环，所以它又是正则环.

11. 由上题及定理9即得.

12. 假定$a\in J$，因为$aa'a=a$，而$a(-a')\in J$，所以R中有元b使

$$-aa'+b-aa'b=0$$

用aa'左乘化简即得$-aa'=0$. 于是$a=0$，所以$J=0$.

13. 假如$\frac{n}{m}+\frac{n'}{m'}+\frac{n'n}{m'm}=0$，那么$nm'+n'(m+n)=0$ 即$\frac{n'}{m'}=\frac{-n}{m+n}$因为$n$是偶数，所以只有$\frac{2k}{m}$是左拟正则元.

14. 假定$x\in N$，如果$1+x\in N$，那么$1\in N$这与假设不合. 所以$1+x$有逆元，即$(1+x)(1+x')=1$，因此x是左拟正则元，于是N是拟正则理想，所以$N\subseteq J$. 再假如J中元有逆元，那么$1\in J$，但1不是左拟正则元，所以J中元都没有逆元. 因此$J\subseteq N$. 于是$J=N$.

15. 因为$eJe\subseteq J$，所以eJe中任意元ere是R的左拟正则元，即$ere+b+bere=0$，因此$ere+ebe+ebe\cdot ere=0$. 所以eRe的根基$J'\supseteq eJe$. 再假如$ere\in J'$，那么$eRe(ere)$是eRe的拟正则左理想，于是对于R中任意元x，$exere$是左拟正则元，所以$xere\cdot e=xere$也是左拟正则元，即$Rere\in J$，所以$ere\in J$，因此$ere\in eJe$，即$J'\subseteq eJe$.

16. 因为$\overline{R}=R-N$是本原环，所以$\overline{R}$中有极大左理想$\overline{M}$使得$(\overline{M}(\overline{R})=\overline{0}$. 即$\overline{r}\overline{R}\subseteq\overline{M}$时$\overline{r}=\overline{0}$，因此$rR\subseteq M$时$r\in N$. 但$N\subseteq M$，所以$(M:R)=N$. 这里$M$显然是$R$的极大左理想.

习　题　8.6

1. 因为交换本原环是域.

习　题　8.7

3. 假设R是本原环，A，B是R的两个理想，如果$AB=0$，$B\neq 0$，因为R是V的稠密环，所以R中只有零元零化V. 因此$BV\neq 0$，于是$BV=V$. 所以$AV=ABV=0$，即$A=0$.

5. 因为$e\neq 0$,所以eV关于D的维数$\geqslant 1$.假定ex,ey是两个线性无关的元,根据稠密定理,R中有元a使$aex=0,aey\neq 0$.因此$ae\neq 0$.命$L_x=\{b\mid b\in L,bx=0\}$,那么$L_x$是$R$的左理想,因为$ae\in L_x,ae\in L$,而$L$是极小,所以$L=L_x$.因此$e\in L_x$即$ex=0$.这与假设不合,所以$eV$关于$D$的维数是1.

名 词 索 引

（以汉字笔画为序）

一 画

二 画

三 画

四 画

五 画

六 画

七 画

八　画

九　画

十　画

十一画

十二画

十三画

十四画

十五画

十六画

十八画